Risk-Based Performance Standards Guidance

Chemical Facility Anti-Terrorism Standards

October 2008
Version 2.4

Homeland Security

FINAL DRAFT

Department of Homeland Security
Office of Infrastructure Protection
Infrastructure Security Compliance Division
Mail Stop 8100
Washington, DC 20528
Website: www.dhs.gov/chemicalsecurity

Table of Contents

Tables

Figures

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT[1] DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a high-risk facility may choose to consider as part of its overall strategy to address the RBPSs. High-risk facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

Overview

In Section 550 of the Homeland Security Appropriations Act of 2007 (P.L. 109-295) (Act), Congress gave the Department of Homeland Security (DHS) regulatory authority over security at high-risk chemical facilities. In the Act, Congress instructed DHS to require all high-risk chemical facilities to complete security vulnerability assessments, develop site security plans, and implement protective measures necessary to meet DHS-defined risk-based performance standards.

Pursuant to its congressional mandate, on April 9, 2007, DHS promulgated the Chemical Facility Anti-Terrorism Standards (CFATS), the interim final regulations setting forth the requirements that high-risk (i.e., "covered") chemical facilities must meet to comply with the Act. Among other things, CFATS establishes eighteen Risk-Based Performance Standards (RBPSs) which identify the areas for which a facility's security posture will be examined, such as perimeter security, access

[1] This document is a "guidance document" under the Office of Management and Budget's *Final Bulletin for Agency Good Guidance Practices* and complies with all of the requirements established in that OMB Bulletin. This is the first guidance document issued on the CFATS RBPS, and does not supersede or replace any other guidance documents related to the CFATS. This Guidance does not create or confer any rights for or on any person or operate to bind the public.

control, personnel surety, and cyber security. To meet the RBPSs, covered facilities[2] are free to choose whatever security programs or processes they deem appropriate, so long as they achieve the requisite level of performance in each applicable area. The programs and processes a high-risk facility ultimately chooses to implement to meet these standards must be described in the Site Security Plan (SSP) that every high-risk chemical facility must develop pursuant to the regulations. It is through a review of the SSP, combined with an on-site inspection, that DHS will determine whether or not a high-risk facility has met the requisite levels of performance established by the RBPSs given the facility's risk profile.

To assist high-risk chemical facilities subject to CFATS in selecting and implementing appropriate protective measures and practices to meet the applicable RBPSs, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document* (Guidance). This Guidance provides DHS's interpretations of the level of performance facilities in each of the risk-based tiers created by CFATS should strive to achieve under each RBPS. It also seeks to help facilities comply with CFATS by describing in greater detail the eighteen RBPSs enumerated in CFATS, and by providing examples of various security measures and practices that could be selected to achieve the desired level of performance for each RBPS at each tier.[3]

Inquiries on RBPS Guidance or Other CFATS Issues

For more information on this Guidance document or the CFATS, feel free to contact DHS via the CFATS Help Desk either via e-mail at csat@dhs.gov or via phone at 866-323-2957, or submit questions via regular mail addressed to Dennis Deziel, Deputy Director, Infrastructure Security Compliance Division, U.S. Department of Homeland Security, Mail Stop 8100, Washington, DC, 20528.

[2] Unless otherwise specifically indicated, the terms "facility" or "facilities" in this document refer to "covered" (i.e., high-risk) facilities as designated under CFATS.

[3] The security measures described in this Guidance document are intended only as examples and for illustrative purposes. These measures are based primarily on experience with facilities in the chemical or related industrial sectors and, as the Guidance makes clear, no covered facility is required to adopt these specific measures in order to satisfy the RBPSs; every covered facility is free to submit alternative measures in its Site Security Plan (or in an Alternative Security Program) for DHS approval. Specific measures that may be appropriate for certain types of facilities (e.g., chemical manufacturing plants, oil refineries) may not be appropriate or necessary for other types of facilities (e.g., universities, hospitals or medical research facilities, agricultural chemical suppliers). DHS expects to cooperate with affected sectors in developing appropriate security measures that will satisfy the RBPSs under the circumstances applicable to facilities in those sectors.

CFATS Risk-Based Performance Standards

Pursuant to Section 550 of the Act, DHS is required to "establish risk-based performance standards for chemical facilities." In 6 CFR §27.230, DHS enumerated the eighteen Risk-Based Performance Standards that covered chemical facilities must meet to be in compliance with CFATS. The eighteen RBPSs are repeated in Table 1.

"Performance standards" have a long and well established history in federal rulemakings.[4] As the Office of Management and Budget has explained, performance standards "state[ ] requirements in terms of required results with criteria for verifying compliance but without stating the methods for achieving required results."[5] Stated differently,

> A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the regulated entity. In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance standard sets a goal and lets each regulated entity decide how to meet it.[6]

By employing performance standards, CFATS allows covered facilities the flexibility to choose the most cost-effective method for achieving a satisfactory level of security based on their risk profile. While providing flexibility, the performance standards used in CFATS nevertheless establish and maintain reasonable thresholds that covered facilities will have to reach in order to gain DHS approval under the regulation.

Table 1: Section 27.230 Risk-Based Performance Standards
(1) Restrict Area Perimeter. Secure and monitor the perimeter of the facility; **(2) Secure Site Assets.** Secure and monitor restricted areas or potentially critical targets within the facility; **(3) Screen and Control Access.** Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including, (i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and (ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;

[4] See Cary Coglianese et al., Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection, 55 Admin. L. Rev. 705, 706-07 (2003).
[5] OMB Circular A-119 (Feb. 10, 1998).
[6] Coglianese, Performance-Based Regulation, 55 Admin. L. Rev. at 709.

Table 1: Section 27.230 Risk-Based Performance Standards

(4) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;

(iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and

(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.

(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;

(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;

(7) Sabotage. Deter insider sabotage;

(8) Cyber. Deter cyber sabotage, including by preventing unauthorized on-site or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems;

(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;

(10) Monitoring. Maintain effective monitoring, communications and warning systems, including

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

(11) Training. Ensure proper security training, exercises, and drills of facility personnel;

(12) Personnel Surety. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

(i) measures designed to verify and validate identity;

(ii) measures designed to check criminal history;

(iii) measures designed to verify and validate legal authorization to work; and

(iv) measures designed to identify people with terrorist ties;

(13) Elevated Threats. Escalate the level of protective measures for periods of elevated threat;

(14) Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

(15) Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials;

(16) Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and

Table 1: Section 27.230 Risk-Based Performance Standards
maintain records of significant security incidents and suspicious activities in or near the site; **(17) Officials and Organization**. Establish official(s) and an organization responsible for security and for compliance with these standards; and **(18) Records.** Maintain appropriate records.

As Section 550 of the Act requires that DHS use "risk-based" performance standards, the level of performance necessary to satisfy each RBPS is dependent on a facility's risk-based tier level. To achieve this, CFATS uses a "tiered" approach, wherein higher tier facilities are expected to meet higher levels of performance than lower tier facilities. See 6 CFR § 27.230(a). Generally speaking, Tier 1 facilities are expected to meet the highest level of performance, with the expected level of performance becoming less stringent as one moves down the tiers. However, for certain RBPSs (e.g., RBPS 17 – Officials and Organization; RBPS 18 – Records), the expected target level of performance is the same for more than one tier.

Regardless of tier level, all high-risk facilities must satisfy all applicable RBPSs. Note, however, that this does not necessarily mean that specific security measures or practices must be implemented for each RBPS. A facility may be able to satisfy an RBPS by the lack of any item on-site that could cause the security issue being addressed by the RBPS. For instance, if a facility has no dangerous chemicals for which theft or diversion is a security issue, then it does not need to implement any additional measures to comply with RBPS 6 – Theft and Diversion. Similarly, if a facility has no computers or other cyber equipment on-site, it does not need to implement any additional measures to comply with RBPS 8 – Cyber. In situations where a facility believes it can satisfy a RBPS without the implementation of any specific security measures or practices, the basis for this belief should be clearly articulated in the facility's Site Security Plan.

How to Use this Guidance Document

This Guidance document was developed to assist covered facilities in complying with the RBPSs established in CFATS. High-risk chemical facilities can use this document both to help them get a sense of what types and combinations of security measures and processes are likely to satisfy a given RBPS for a facility at their tier level, and to help them identify and select processes, measures, and activities that they may choose to implement to secure their facility. However, this Guidance document does not require any covered facility to adopt any specific measure or practice; a covered facility is free to adopt and implement any security measures or practices appropriate to its circumstances, so long as DHS determines that those measures are adequate to meet the applicable RBPS.

The programs and processes a high-risk facility ultimately chooses to implement to meet these standards must be described in the SSP that every high-risk chemical facility must develop pursuant to the regulations. 6 CFR §§ 27.225, 27.245. It is through a review of the SSP, combined with an on-site inspection, that DHS will determine whether a facility has met the requisite level of performance given its risk profile. Information contained within the SSP, as well as information exchanged between the facility and DHS staff and/or inspectors during the inspection process, generally is considered Chemical-terrorism Vulnerability Information (CVI) under the CFATS rule, and should only be shared with those who have a need to know and have been certified by DHS as authorized users of CVI. See 6 CFR § 27.400.

In addition to the overview and information on how to use this guidance document, the introductory portion of the document contains some general considerations for high-risk facilities selecting security measures to comply with CFATS. Following the introductory portion of the document, the chapters of the Guidance document focus in order on the eighteen RBPSs. Each of those chapters contains three primary sections:

- *Introductory Overview* – A brief explanation of the RBPS and what the RBPS is intended to accomplish. The RBPSs purpose is detailed in this section, and any terms of art used in the guidance relating to the RBPS will be defined here as well.

- *Security Measures and Considerations* – A discussion of some potential security measures and/or activities that may be useful in meeting the goals of the RBPS, as well as some issues covered facilities may wish to consider when selecting an appropriate combination of measures and practices to address an RBPS. This will include (1) an overview of the categories of security measures and/or activities that are recommended for consideration in identifying actions to meet the RBPS, (2) specific security measures and/or practices that a facility may want to implement or may already be implementing that could help it meet the RBPS, and (3) security and design considerations that a facility may want to take into account when determining what measures and/or practices to undertake. Additional detailed information on various protective activities and security and design considerations

can be found in Appendix C. Note that the security measures listed in each chapter and in Appendix C are neither mandatory nor necessarily the "preferred solution." Nor are they the complete list of potential activities from which a facility can choose to meet each RBPS. Rather, they are some example measures that a facility may choose to implement as part of its overall strategy to address the RBPSs. Facility owners/operators may consider other solutions based on the facility, its security risks, and its security program, so long as the suite of measures implemented achieve the targeted level of performance.

- *RBPS Metrics* –In tabular format, a statement of specific performance objectives (i.e., metrics) that DHS feels would be appropriate goals for facilities to consider in demonstrating compliance under each RBPS. The RBPS Metrics include a *summary* or high-level statement of the level of performance relative to each RBPS that DHS generally would expect to find at a compliant facility in that tier, and individual *metrics*, or specific targets, as examples that a facility may seek to achieve for specific, individual aspects of each RBPS. A summary and set of individual metrics is provided for each RBPS and each risk-based tier.

  Note that the metrics included within the RBPS guidance document are for exemplary purposes only, and a facility need not necessarily meet any or all of the individual metrics to be in compliance with CFATS. Rather, the summary and individual metrics are meant to help a facility identify gaps in its own security posture and potentially mitigating activities by understanding the levels of performance that a compliant facility typically will be able to demonstrate. While a facility meeting all of the metrics is likely to be in compliance with the CFATS RBPS, the failure to meet any particular metric or summary level – or the substitution of alternative measures – does not automatically mean that a facility will not be in compliance with CFATS. In actuality, the levels of performance that a facility must achieve to be in compliance will be unique for each facility based on its risk profile, and compliance status will be examined comprehensively on a case-by-case basis, rather than by measuring attainment of a finite list of prescribed objectives. Facilities may be able to demonstrate compliance with the RBPS through the use of other measures which DHS determines to be appropriate.

In addition to the three primary sections described above, many chapters contain a text box describing the attack scenarios a facility should consider when determining what security measures and/or practices to implement to meet the RBPS. Note that these are not "Design Basis" threats, and there is no specific requirement for a facility to be able to defend itself from each of these types of threats. Rather, the attack scenarios are analytical devices, supporting the evaluation of a facility's security and enabling DHS to conduct comparative risk analysis across the sector. Not all attack scenarios apply to every RBPS. Table 2 below maps out which attack scenarios apply to which RBPSs. In the Table, an X indicates that the RBPS is potentially applicable to the scenario, a blank indicates that the RBPS is not applicable to the scenario, and a solid box indicates that the RBPS is indirectly applicable to the scenario. For those RBPSs where none of the attack scenarios are directly applicable, no attack scenario text box is included.

Table 2: Applicable Attack Scenarios and RBPS

	1) Restrict Area Perimeter	2) Secure Site Assets	3) Screen and Control Access	4) Deter, Detect, and Delay	5) Shipping, Receipt, and Storage	6) Theft and Diversion	7) Sabotage	8) Cyber	9) Response	10) Monitoring	11) Training	12) Personnel Surety	13) Elevated Threats	14) Specific Threats, Vuls or Risks	15) Reporting Significant Sec Events	16) Significant Sec Incidents \Activities	17) Officials and Organization	18) Records
Aircraft									X									
Assault Team	X	X	X	X	X				X			X						
Maritime	X			X					X									
Sabotage	X	X	X	X	X		X	X	X			X						
Stand-Off	X	X	X	X	X				X									
Theft/Diversion	X	X	X	X	X	X		X	X			X						
Vehicle Borne Improvised Explosive Device (VBIED)	X	X	X	X	X				X			X						

Following the chapters on the eighteen RBPSs, a number of appendices have been included to provide additional assistance to covered facilities in both understanding this Guidance document and in complying with the RBPS contained in the CFATS regime. These include: (a) acronyms used in the Guidance document (Appendix A); (b) a compilation of all the RBPS Metrics by tier (Appendix B); and (c) additional information on Security Measures and Considerations that a facility may choose to use to help meet one or more of the RBPSs, including lists of additional resources by topical area (Appendix C).

General Considerations for Selecting Security Measures to Comply with CFATS

To assist high-risk facilities in selecting a suite of security measures and activities that both meet the CFATS performance standards and are tailored to the unique considerations associated with a facility, DHS offers the following general considerations.

The Non-Prescriptive Nature of Risk-Based Performance Standards. First and foremost, when selecting what security measures and activities to implement to comply with CFATS, a high-risk facility's owners or operators should keep in mind that because CFATS uses a performance-standard based approach, DHS is not requiring that any specific measure or activity be used. In fact, Congress has expressly prohibited DHS from disapproving a Site Security Plan based on the presence or absence of a particular security measure. Accordingly, the measures and activities listed in each chapter and in Appendix C are neither mandatory nor necessarily the "preferred solution." Nor are they the complete list of potential activities from which a high-risk facility must choose to meet each RBPS. Rather, they are some example measures that a facility may choose to implement as part of its overall strategy to address the RBPSs. Facility owners/operators may consider other solutions based on the facility, its security risks, and its security program, so long as the suite of measures implemented achieve the targeted level of performance.

The Impact of the Nature of the Security Issue Underlying the Facility's Risk Determination. Preliminary screening requirements for initially determining if a facility is high-risk under CFATS are triggered by the possession, in specified quantities, of certain types of chemicals of interest (COI), including:

- chemicals with the potential to create a toxic cloud or vapor cloud explosion that would affect populations within and beyond the facility if intentionally released (i.e., release-toxic and release-flammable chemicals of interest (COI)[7]);
- chemicals with the potential to affect populations within and beyond the facility if intentionally detonated (i.e., release-explosive COI);
- chemicals that could be stolen or diverted and used in explosives (EXP) or Improvised Explosive Devices (IEDs) (i.e., theft/diversion-EXP/IEDP);
- chemicals that could be stolen or diverted and used directly as chemical weapons (CW) or weapons of mass effect (WME), or easily converted into CW(i.e., theft/diversion-WME and theft/diversion-CW/CWP COI); and

[7] For the purposes of illustration and guidance, many of the examples provided in this document refer to security issues and security measures related to chemicals of interest, as listed in 6 CFR Part 27, Appendix A. However, actual security issues and measures that must be addressed in a Site Security Plan to satisfy the risk-based performance standards at any particular facility will not necessarily be limited to chemicals of interest.

- Possession of chemicals that, if mixed with other readily-available materials, have the potential to create significant adverse consequences for human life or health (i.e., sabotage/contamination COI). [8]

While high-risk facilities must address all of the RBPSs, regardless of the security issue(s) associated with possession of the COI, facility owners and operators should keep in mind those security issues when designing the security measures for the facility's SSP. Different security measures or activities may be more or less effective depending on the specific security issues. In the following paragraphs, the Department discusses three security issues along with examples of specific security measures and activities that facilities may want to consider if they face that particular security issue:[9]

- Release COI. For high-risk facilities whose primary security issue is possession of a release COI, the primary security goal often is the prevention of an intentional, uncontrolled release of the COI. This presents a different challenge than faced by the other types of COI for two main reasons: (1) a successful physical attack on a release COI can take place from off-site, and (2) the harmful health and human life consequences typically will begin on-site.

  In light of the first unique concern, facilities with release COI could use certain specific protective measures or activities that facilities with only theft/diversion or sabotage security issues would not typically use, such as:

  - Strong vehicle barriers surrounding the release COI;
  - Elimination of clear lines of sight to the release COI;
  - Standoff distance around the release COI;
  - Limitations on on-site parking and additional parking security measures; and
  - Refusal to accept unannounced shipments or off-site staging of unannounced shipments until they can be verified.

  The second main concern (i.e., that the potential harmful consequences will almost always begin at a source on-site) suggests a need for certain specific activities that would be more beneficial for facilities with release COI than facilities with other types of security issues, such as:

  - A comprehensive emergency response and crisis management plan;

[8] The Department also has the authority to declare facilities to be high-risk based on the impact a terrorist incident could have on national security or critical economic assets ("economic or mission criticality"). As of the date of publication of this guidance document, the Department has not yet listed any chemicals of interest under CFATS, or made any high-risk determinations, on that basis. If, in the future, the Department uses either economic criticality or mission criticality as a basis for designating facilities as high-risk, the Department likely will update this document to provide additional guidance to those facilities.

[9] Note that there are many security measures or activities that could be considered parts of a good security posture regardless of the security issue driving the facility's risk. These include, but are not limited to, access control systems, visitor security measures, a security force, monitoring and surveillance systems, cyber security, personnel surety (i.e., background checks), a clearly defined security organization, security equipment monitoring and testing, and security awareness training.

- An on-site emergency notification system;
- Safe shutdown procedures for processes or areas using or containing the release COI;
- Extensive training, including exercises and drills (involving local first responders when possible), on responding to an uncontrolled release.

- Theft/Diversion COI. For facilities whose security issues are related primarily to the possession of theft/diversion COI, the primary security focus is not preventing a successful attack on the facility, but rather preventing the acquisition of the COI by an adversary through theft or deception. Because of this different focus, some of the measures that are central to security at facilities with release COI, such as vehicle barriers, stand-off distance, parking security measures, and vehicle inspections upon entry, may not be as critical to facilities with only theft/diversion COIs. Instead, for facilities with theft/division COI, the primary means to prevent theft or diversion include inventory control systems that can monitor and/or track theft/diversion of COI, procedures that make it more difficult to steal or divert the chemicals, and physical measures that make the actual movement of such chemicals more difficult. Specific measures that often could be considered part of good security measures for facilities with theft/diversion COI include:

  - Intensive product stewardship efforts that include a "know your customer" program and verification of receipt of shipments;
  - Inventory control systems and/or relational databases that provide tracking of the quantity and physical location of all theft/diversion COI;
  - Restricted access to areas where theft/diversion COI is located;
  - Use of the "two-man rule" or constant monitoring of restricted areas to ensure that no person is provided access to theft/diversion COI alone or unmonitored
  - Individual and vehicle inspections upon egress from areas containing theft/diversion COI;
  - Locked racks or other tamper-evident, physical means of securing man-portable containers of COI (e.g., chains and locks; tamper-resistant seals; movement alarms)
  - Cyber security for cyber systems involved not only in processes physically involving the theft/diversion COI, but also in business systems that support the sale, transfer, or distribution of the theft/diversion COI;
  - Background checks not only on those individuals with physical access to critical assets (e.g., the theft/diversion COI), but also on employees who may never physically handle the COI but who are responsible for arranging the sale, transfer, or distribution of those COI or who have access to the critical cyber systems controlling the sale, transfer, or distribution of the COI.

  Additionally, while facilities with release COI generally should have a wide security footprint surrounding areas where the release COI is located, facilities with theft/diversion security issues will often find it more cost-effective to focus their efforts primarily on securing the specific buildings or locations where the theft/diversion COI is manufactured, processed, used, or stored.

- Sabotage COI. The primary security goal for facilities that possess sabotage/contamination COI is to prevent tampering with the COI. Because the consequences from tampering with sabotage COI typically occur well after the attack, the adversary is more likely to use

deception rather than brute force. Accordingly, some of the more important measures for preventing sabotage typically include:

- a strong personnel surety program for all employees with access to the COI;
- a good access control system;
- visitor security measures;
- constant monitoring and surveillance of the COI and processes involving the COI;
- tamper-resistant storage of the COI.

The Impact of the Type of Facility and Its Physical and Operating Environments. Just as the security issue(s) at a facility affect the suite of measures the facility will employ to meet the RBPSs, different types of facilities may vary widely in the types and level of security measures that are appropriate for their physical and operating environments. For instance, DHS would not expect a university or medical research facility to implement the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues. The measures that a covered facility selects and describes in its Site Security Plan should be tailored not only to the facility's tier level and security issues, but also to the type of facility and its physical and operating environments.

An Individual Measure May Support Achievement of Multiple Risk-Based Performance Standards. Protective measures and processes may be but do not have to be tailored to individual RBPSs. In many cases, a single protective measure or process can help a facility meet the targeted levels of performance for a variety of RBPSs at once. For instance, depending on how they are designed, perimeter barriers can assist a facility in meeting RBPS 1, 2, 3, 4, and 6. Similarly, a security force, while alone likely insufficient to meet any single RBPS entirely, can help a facility meet the targeted level of performance for virtually every RBPS.

Layered Security/Combining Barriers and Monitoring to Increase Delay. Completely adequate perimeter security is rarely achievable through the deployment of a single security barrier or monitoring system; rather an optimal security solution typically involves the use of multiple protective measures providing "layers of security." Layering of security measures can be achieved in many different manners, such as:

- Incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems with procedural security measures, such as procedures guiding how a security should respond to an incident)
- Using multiple lines of detection used to achieve protection-in-depth at critical assets
- Using complementary sensors with different means of detection (e.g., a closed circuit television (CCTV) and an intrusion detection system) to cover the same area.

A layered approach to perimeter security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

Asset-Specific vs. Facility-Wide Measures. For many facilities, their level of risk will be driven by a finite number of assets contained within the facility.[10] When this occurs, a facility may want to consider employing asset-specific measures (as opposed to facility-wide measures) to meet the risk associated with the highest risk asset(s). For example, if a ten acre facility has a single, finite Tier 2 hazard and the rest of the assets on-site are Tier 4 risks or not high-risk, to meet RBPS 1, it could be more cost-effective for the facility to employ perimeter barriers meeting Tier 2 standards around only the Tier 2 asset, with perimeter barriers meeting Tier 4 standards around the entire facility's perimeter, than it would be to employ perimeter barriers meeting Tier 2 around the entire facility.

[10] A facility's tier level is the tier level assigned to the highest risk asset on-site. For example, if a facility has a building located on-site that contains a Tier 2 theft hazard, and twenty storage vessels, each of which is a Tier 4 release hazard, the facility is a Tier 2 facility despite the significantly larger number of Tier 4 assets on-site. In such a scenario, while the Tier 2 theft hazard must be protected to Tier 2 performance levels, and the facility must employ Tier 2 measures at the macro level, the measures directed at the Tier 4 assets need only meet Tier 4 performance standards.

RBPS 1 – Restrict Area Perimeter

RBPS 1 - Restrict Area Perimeter - Secure and monitor the perimeter of the facility.

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

The "Restrict Area Perimeter" RBPS addresses the need to provide for a controlled perimeter surrounding the facility or, optionally, the critical assets only if the restricted area is defined to be less than the entire facility. The purpose of the RBPS 1 – Restrict Area Perimeter is to reduce the likelihood of unauthorized persons accessing the facility for malicious purposes such as theft, sabotage, or intentional release of chemicals of interest. By securing and monitoring the perimeter of the facility, facility personnel can more easily and effectively control who enters and leaves the facility, both on foot and in vehicles, and are better able to detect, delay, defend against, and respond to individuals or groups who seek unauthorized access to the facility. A well-secured perimeter additionally will help to deter intruders from seeking to gain access to the facility or from launching attacks from the area immediately outside a facility's perimeter.

Restricting the area perimeter involves two fundamental aspects – 'securing' the restricted area and 'monitoring' the restricted area. These two concepts, described below, act in unison to allow a facility to deter, detect, and defend against breaches of the facility perimeter.

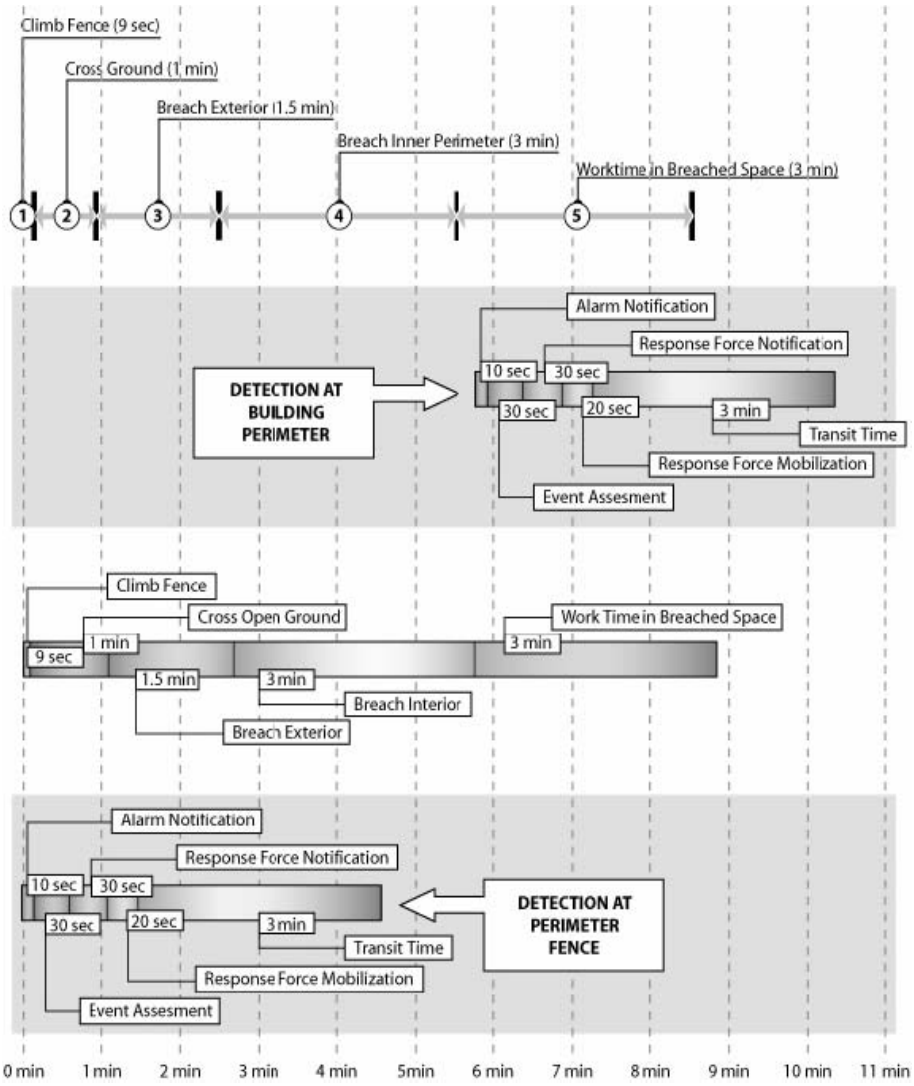
- **Secure** – In the restrict area perimeter context, 'secure' means physically limiting the accessibility of the facility such that there is a low likelihood of an adversary successfully breaching the facility perimeter or using the area immediately outside of the facility's perimeter to launch an attack. Securing a facility is frequently done using one or more layers of physical barriers (e.g., fencing, man-made obstacles, natural obstacles) and/or guard forces. As guard forces are not a practical solution for many facilities to fully address this RBPS, it is anticipated that physical barriers will commonly be used.

- **Monitor** – In the restrict area perimeter context, 'monitor' refers to the need to have domain awareness of the perimeter including the areas immediate beyond the perimeter (the "buffer zone") and the area just inside the perimeter. Frequently this is accomplished by using intrusion detection systems integrated with other electronic surveillance systems, often in conjunction with a security force, that monitor the facility perimeter to deter, detect, communicate and evaluate the presence of unauthorized persons or vehicles, or unauthorized activities.

Figure 1 shows how securing and monitoring a facility's perimeter through barriers or other delay mechanisms could help successfully prevent adversaries from reaching a target inside a facility.[11] In Figure 1, the steps needed for a hypothetical attack and the time each step would take is mapped against two facilities—one without perimeter barriers and monitoring equipment, and one with perimeter barriers and/or monitoring equipment. In the first hypothetical, at the facility without perimeter barriers or monitoring equipment, initial detection of the attack is not made until the interior wall (or fence) of the critical asset has been breached, well after the adversaries have entered the facility. Because initial detection of the attack does not occur until six minutes into the attack, response forces do not arrive on the scene until after some compromise of the critical asset has been achieved. In the second hypothetical, however, thanks to the perimeter barriers and monitoring equipment, initial detection is made at the fence line, and response forces are able to arrive and intervene before the critical assets located at the interior of the facility are compromised.

[11]Department of Defense, Unified Facilities Criteria (UFC) UFC 4-021-02NF, Electronic Security Systems, October, 2006.

Figure 1 – Barriers/Detection Performance (Source: Sandia)



This hypothetical attack could involve a disruption of an infrastructure asset the facility is dependent on and is at the perimeter of the facility, or it may involve penetration of the facility to get near enough to an interior target asset, such as a chemical of interest, to cause the desired damage considering the weapon and its impact area. The goal of an attack may also be to commit a theft, in which case an adversary will need to get near enough to the asset to directly remove the targeted substances, such as man-portable quantities of a chemical of interest. Whatever the case, when designing a perimeter security system, a facility may want to consider all relevant potential terrorist attack scenarios based on the physical juxtaposition of the target asset (such as a COI), the perimeter, and the related adversary considerations.

Security Measures and Considerations for Restricting Area Perimeter

Security Measures

Effective measures for securing a facility's perimeter often involve some combination of (1) perimeter barriers, (2) intrusion detection systems or other types of monitoring, (3) lighting, and (4) protective forces.

Perimeter Barriers

Perimeter barriers provide both physical obstacles and psychological deterrents to unauthorized entry, delaying or preventing forced entry. Example barriers that could be implemented in support of RBPS 1 include, but are not limited to:

- Human barriers (e.g., fences, gates)
- Vehicle barriers (e.g., jersey barriers, berms, bollards, planters)
- Natural or landscaping barriers (e.g., hedge rows, rocks, timber, water)
- Walls (e.g., brick, cinder block, poured concrete)

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Restrict Perimeter Access performance standards, a facility might consider the following potential attack scenarios:

- Assault Team
- Maritime
- Sabotage
- Stand-Off
- Theft/Diversion
- VBIED

Perimeter barriers can be used in a variety of ways to restrict the area perimeter and increase overall facility security, including:

- Controlling vehicular and pedestrian access
- Providing channeling to facility entry-control points
- Delaying forced entry
- Protecting critical assets

Additional information on each of these types of barriers, including specific examples of each, can be found in Appendix C, along with factors a facility may wish to consider when determining which, if any, perimeter barriers to implement.

Monitoring

Monitoring and detection equipment are key components of many effective perimeter security postures. Often, facilities will monitor for security events through a combination of human oversight and one or more electronic sensors or other intrusion detection system (IDS) components interfaced with electronic entry-control devices and alarm reporting displays. Typically, when a sensor or other IDS component identifies an event of interest, an alarm notifies security, who then will assess the event either directly by sending persons to the location of the event or remotely by personnel evaluating sensor inputs and surveillance imagery.

There are many possible configurations of IDS components that together could satisfy the RBPS for securing and monitoring the facility perimeter. An effective IDS for a high-risk chemical facility could, for example, use a combination of two or more of the following items:

- Fence-mounted, beam, or open area sensors (e.g., vibration detection sensors, video motion detection, infrared sensors, acoustic sensors)
- Remote surveillance (e.g., CCTV cameras, thermal images, Internet Protocol (IP) cameras)
- Human-based monitoring via protective forces.

To increase the reliability of a monitoring system, an owner/operator may elect to deploy multiple interactive, redundant, or sophisticated sensors or counter-measures at high-risk locations with the understanding that increased reliability also extends to the functional capabilities of the data-transmission system.

An integrated perimeter security system may include not only the sensors, remote surveillance, and human monitoring, but also the means of transmitting data gathered by the monitoring system, and a reporting process for monitoring, controlling, and displaying information on security events. When such electronic components are included in the perimeter monitoring system, the owner/operator may wish to locate alarm reporting devices and video monitors in a command and control center. Routine functions carried out in a control center may include selecting and assessing alarms; controlling video recording, playback, and display; checking the status of system components; changing sensor states; conducting some system self-tests; and controlling door locks.

Additional information on monitoring equipment, IDS elements, and command and control centers, can be found in Appendix C, along with factors a facility may wish to consider when determining which, if any, sensors or remote surveillance to deploy.

Security Lighting

Security lighting can help to both deter attempts at penetrating a facility's perimeter and assist in the monitoring and detection of any such attempts. Inadequate lighting can make it more difficult to monitor a perimeter and detect attempts to breach the perimeter either directly through human protective forces, or through certain types of monitoring and intrusion detection systems, such as CCTVs. Due to the increased likelihood of detection based on appropriate security lighting, maintaining a well lit facility perimeter also can help deter adversaries from attempting to breach that perimeter.

A wide variety of different types of security lighting is available for implementation at facilities. When determining if security lighting is an appropriate part of a facility's security posture and what type of lighting to choose, a facility should consider such items as local weather conditions, available power sources, grounding, and interoperability with and support to other monitoring and detection systems, such as CCTVs.

Protective Forces

Protective forces are often used to enhance perimeter security and provide a means of deterrence, detection, delay, and response. Such forces can be proprietary or contracted, and can be armed or unarmed. Protective forces can be used in a variety of ways, including standing post at critical assets, monitoring critical assets using remote surveillance, or conducting roving patrols on a documented schedule that specifically includes identified targets, processes, or assets. Protective forces may be qualified to interdict adversaries themselves, or simply to deter and detect suspicious activities and to then call local law enforcement to provide an interdiction.

No matter how they are deployed, protective forces alone frequently do not provide sufficient perimeter security. Accordingly, if a facility employs protective forces, they may need to be used in combination with one or more of the other measures listed above to provide an appropriate level of security to meet the Restrict Area Perimeter performance standard.

Security Considerations

Layered Security/Combining Barriers and Monitoring to Increase Delay

Completely adequate perimeter security is rarely achievable through the deployment of a single security barrier or monitoring system; rather an optimal security solution typically involves the use of multiple protective measures providing "layers of security." Layering of security measures can be achieved in many different manners, such as:

- Incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems with procedural security measures, such as procedures guiding how a security should respond to an incident)
- Using multiple lines of detection used to achieve protection-in-depth at critical assets
- Using complementary sensors with different means of detection (e.g., a CCTV and an intrusion detection system) to cover the same area.

A layered approach to perimeter security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

Securing Entire Perimeter vs. Securing Individual Asset

Depending on the size and location of the asset or assets driving a tier's risk, it may be more cost-effective to focus security on the asset(s) rather than the entire perimeter. For instance, if a facility is a large facility (e.g., covering 10 square miles) that has a single, relatively small Tier 1 asset (e.g.,

a single building or container), it could be significantly more cost-effective to apply Tier 1 level perimeter barriers solely around the perimeter of the Tier 1 asset rather than the entire facility. Accordingly, an owner/operator may wish to consider the benefits and costs related to completely enclosing a large facility within a single perimeter versus implementing multiple smaller restricted area perimeters.

Additional discussion on the pros and cons of securing an entire perimeter versus securing the individual high-risk assets contained therein is discussed in the Introduction. For performance objectives related to securing individual assets, an owner/operator should refer to RBPS 2 – Secure Site Assets.

Physical and Environmental Considerations

When determining the selection and layout of perimeter security components, a facility owner/operator should take into consideration the physical and environmental characteristics of his or her facility. Important *physical considerations* for evaluating the cost-effectiveness of perimeter countermeasures include:

- Perimeter length and convolution
- Terrain and urbanization
- Adjacent facilities and transportation corridors
- Approach angles and vehicle speeds
- Availability of supporting infrastructure

In addition to the physical considerations listed above, *environmental factors* also should be considered when making decisions regarding perimeter security, as certain environmental conditions can significantly affect sensor and lighting performance. For example, certain sensors or other IDS components that have near perfect detection capabilities during good weather might be subject to unacceptably high levels of false alarms during inclement weather (e.g., fog, rain, wind). Similarly, security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather. Accordingly, an owner/operator should consider the impact of environmental conditions when making determinations regarding security lighting and sensors or other IDS components.

Additional discussion on physical and environmental factors to take into considerations when making security decisions can be found in Appendix C.

Command and Control Considerations

Many perimeter security measures, such as intrusion detection systems or CCTV systems, consist of various hardware and software elements that can only be effectively operated or monitored by trained personnel, and owner/operators often will locate these functions in a command and control center. When designing command and control centers, owner/operators should consider merging security monitoring and reporting systems with other systems, such as fire engineering reporting systems or process control. Technical merger of an active security system and a passive fire system may facilitate a common set of operational procedures (e.g., reporting, training, and emergency response), and prove a more cost-effective approach to overall facility safety and security management.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 – Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has an extremely vigorous perimeter security and monitoring system that enables the facility to thwart most adversary penetrations and channel personnel and vehicles to access control points; including a perimeter intrusion detection and reporting system with multiple additive detection techniques that can demonstrate an extremely low probability that perimeter penetration would be undetected.	The facility has a vigorous perimeter security and monitoring system that enables the facility to thwart or delay most adversary penetrations and channel personnel and vehicles to access control points; including a perimeter intrusion detection and reporting system that can demonstrate a very low probability that perimeter penetration would be undetected.	The facility has a perimeter security and monitoring system that enables the facility to delay a significant portion of attempted adversary penetrations and channel personnel and vehicles to access control points; including a perimeter intrusion detection and reporting system that can demonstrate a low probability that perimeter penetration would be undetected.	The facility has a perimeter security and monitoring system that enables the facility to delay a portion of attempted adversary penetrations and channel personnel and vehicles to access control points; including a system to monitor and report unauthorized penetrations of the facility perimeter.

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 – Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 1.1 – Perimeter Security	The facility has an extremely vigorous, high integrity system to secure the perimeter that severely restricts or delays any attempts by unauthorized persons to gain access to the facility. To achieve this standard, a facility could, for example, use the following: • An exterior perimeter fence that is a security fence or equivalent barrier that meets industrial consensus standards. • A clear zone on either side of the fence that allows persons to be detected at the boundary. Where vehicles can access either side of the boundary, the clear zone is wide enough to allow detection of the presence of vehicles.	The facility has a vigorous, high integrity system to secure the perimeter that would give unauthorized persons a very low probability of gaining access to the facility. To achieve this standard, a facility could, for example, use the following: • An exterior perimeter fence that is a security fence or equivalent barrier that meets industrial consensus standards. • A clear zone on either side of the fence that allows persons to be detected at the boundary. Where vehicles can access either side of the boundary, the clear zone is wide enough to allow detection of the presence of vehicles.	The facility has a system to secure the perimeter that would give unauthorized persons a low probability of gaining access to the facility. To achieve this standard, a facility could, for example, use a single security barrier, such as: • An exterior perimeter fence that is a security fence or equivalent barrier that meets industrial consensus standards.	The facility has a system to secure the perimeter that reduces the possibility of access of to the facility by unauthorized persons. To achieve this standard, a facility could, for example, use a single security barrier, such as: • An exterior perimeter fence that is a security fence or equivalent barrier that meets industrial consensus standards.

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 – Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 1.2 – Vehicle Barriers	Vehicles would have a very low likelihood of accessing the target by force anywhere along the entire perimeter where vehicle attack is a possible mode of attack. To achieve this, a facility could, for example, use aggregate barriers with a minimum of a Department of State (DOS) K8 vehicle barrier rating or equivalent (desired barrier rating can vary based on maximum attainable vehicle speed at the barrier). Examples include: • Vehicle deterrence measures such as bollards, landscaping, berms, ditches, drainage swale, or buried concrete anchors retaining anti-vehicle cable wherever the perimeter is accessible to a vehicle. • Entrances equipped with traffic control systems to slow incoming traffic, such as serpentine barriers outside the gate.	Vehicles would have a low likelihood of accessing the target by force anywhere along the entire perimeter where vehicle attack is a possible mode of attack. To achieve this, a facility could, for example, use aggregate barriers with a minimum of a DOS K8 vehicle barrier rating or equivalent (desired barrier rating can vary based on maximum attainable vehicle speed at the barrier). Examples include: • Vehicle deterrence measures such as bollards, landscaping, berms, ditches, drainage swale, or buried concrete anchors retaining anti-vehicle cable wherever the perimeter is accessible to a vehicle. • Entrances equipped with traffic control systems to slow incoming traffic, such as serpentine barriers outside the gate.	Vehicles would have a reduced likelihood of accessing the target by force anywhere along the entire perimeter where vehicle attack is a possible mode of attack. To achieve this, a facility could, for example, use active or passive barriers with a minimum DOS K4 vehicle barrier rating or equivalent (desired barrier rating can vary based on maximum attainable vehicle speed at the barrier) at perimeter control points where vehicles normally enter and leave the facility and other anti-vehicle barriers such as ditches, revetments, or other man-made or naturally occurring barriers for the remainder of the perimeter where vehicle attack is a possible mode of attack.	Vehicles would have a reduced likelihood of accessing the target by force at the perimeter control points where vehicles normally enter and leave the facility. To achieve this, a facility could, for example, use anti-vehicle barriers such as ditches, revetments, or other man-made or naturally occurring barriers.
Metric 1.3 – Standoff Distance	Sufficient vehicle standoff distance or alternative protective means are provided to ensure that vehicle-borne improvised explosive devices will not cause a breach of containment resulting in an uncontrolled release of a release chemical of interest from the nearest point of attack.		N/A	
Metric 1.4 – Monitoring and Surveillance	The facility has an extremely reliable perimeter monitoring system which continuously monitors the entire length of the facility perimeter, allows for the identification and evaluation of an intrusion in real time, and provides notification of intrusion to a continuously manned location. In the context of this metric, "real time" means that an adverse act	The facility has a very reliable perimeter monitoring system which continuously monitors the entire length of the facility perimeter, allows for the identification and evaluation of an intrusion in real time, and provides notification of intrusion to a continuously monitored location. In the context of this metric, "real time" means that an adverse act	The facility has a reliable perimeter monitoring system that allows for the identification of the presence of an intrusion in real time for the area(s) containing the target asset(s). In the context of this metric, "real time" means that an adverse act likely is detected and reported to responders in a timely manner. "Reliable" means that the monitoring	The facility has a monitoring system that allows for the identification of the presence of an intrusion in the area(s) containing the target asset(s). To achieve this, a facility typically could, for example, use security patrols of the facility or an integrated monitoring system that provides intrusion detection and video surveillance around

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 – Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	virtually always is detected and reported to responders at the time of occurrence. "Extremely reliable" means that the monitoring system is operable during all anticipated conditions, including complete darkness, twilight, inclement weather, and loss of power; with monitoring system components designed, laid-out, and constructed to avoid common cause/dependent failures and provide redundant signal processing equipment where digital signal processing is used. To achieve this, a facility typically could, for example, use an integrated, multi-sensor system that: • Provides intrusion detection and video surveillance around 100% of the perimeter or 100% of the restricted area around the designated COI or any other target assets. • Whose images or other output are continuously monitored by a dedicated person, software, or other detection methods used in conjunction with the system. • Has emergency back up power and/or an equivalent written contingency procedure. • General area as well as access portal (face view) CCTV surveillance at all gates.	most likely is detected and reported to responders at the time of occurrence. "Very reliable" means that the monitoring system is operable during ambient light, inclement weather, and fluctuating power conditions; with monitoring system components designed, laid-out, and constructed so as to avoid common cause/dependent failures and provide redundant signal processing equipment where digital signal processing is used. To achieve this, a facility typically could, for example, use an integrated monitoring system that: • Provides intrusion detection and video surveillance around designated COI or other target assets. • Whose images or other output are continuously monitored by a dedicated person, software, or other detection methods used in conjunction with the system. • Has emergency back up power and/or an equivalent written contingency procedure.	system is be operable during ambient light conditions. To achieve this, a facility typically could, for example, use an integrated monitoring system that: • Provides intrusion detection and video surveillance around designated COI or other target assets. • Has emergency back up power and/or an equivalent written contingency procedure.	designated COI or other target assets, is fully operable during all lighting conditions.

RBPS 2 – Secure Site Assets

RBPS 2 - Secure Site Assets - Secure and monitor restricted areas or potentially critical targets within the facility.

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

The purpose of RBPS 2 – Secure Site Assets is to secure and monitor restricted areas or potentially critical targets within the facility. Critical targets may include not only locations where chemicals of interest are manufactured, stored, or used, but also other sensitive targets such as process controls, security operations centers, and critical cyber systems. Similar in many respects to RBPS - 1, this performance standard focuses on the protection and monitoring of critical assets and chemicals of interest that are located within a covered facility's perimeter. This RBPS also addresses malevolent acts perpetrated by insiders or insiders in collusion with outsiders, as well as internal security controls that provide additional deterrence, detection, and delay to facilitate timely response to security events.

Securing facility assets involves two fundamental aspects–'securing' the restricted area and 'monitoring' the restricted area. These two concepts, described below, act in unison to allow a facility to deter, detect, and defend against unauthorized release, theft, or sabotage of the critical asset.

- **Secure** – In the secure site assets context, 'secure' means physically limiting the accessibility of the asset to reduce the likelihood of unauthorized release, theft, or sabotage. Securing an asset is frequently done using one or more layers of physical

barriers (e.g., fencing, man-made obstacles, natural obstacles) and/or guard forces. As guard forces are not a practical solution for many facilities to fully address this RBPS, it is expected that physical barriers will commonly be used.

- **Monitor** – In the restrict area perimeter context, 'monitor' refers to the need to maintain regular surveillance or close observation over restricted areas and critical assets containing chemicals of interest to detect, evaluate, and communicate the presence of unauthorized persons or activities. frequently this is accomplished by using intrusion detection systems integrated with other electronic surveillance systems, often in conjunction with a security force, that monitor the restricted areas or critical assets to deter, detect, communicate and evaluate the presence of unauthorized persons or vehicles, or unauthorized activities.

Often the facility protective system is organized in depth, containing an integrated suite of mutually supporting security elements that may include:

- Physical measures, such as barriers, lighting, and human observation, integrated as needed with technical security measures and monitoring systems.
- Procedural measures, including controls in place before an incident occurs coupled with those employed in response to an incident.

The combination of protective systems frequently provides defense in depth to secure critical assets within restricted areas from malevolent acts perpetrated by insiders, outsiders, or insiders in collusion with outsiders.

Adequately securing facility assets often depends upon the overlapping principles that deter, detect, delay, and respond to unauthorized acts or individuals. A potential adversary, especially an insider, may perceive the risk of getting caught to be a significant factor in deterring his malevolent act. The effectiveness of deterrence varies with the adversary's refinement, the attractiveness of the asset, and the complexity of the attack scenario. The protective system depends on detection measures (human, electro-mechanical, or both) that sense or perceive (detect) an undesired or unauthorized action, assessing that detection, delaying the adversary, and communicating the event to response forces. Effective integrated protection systems that secure facility assets frequently provide all of these capabilities.

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Secure Site Assets performance standards, a facility might consider the following potential attack scenarios:

- Assault Team
- Sabotage
- Stand-Off
- Theft/Diversion
- VBIED

Protective measures or additional controls are used to detect unauthorized presence; observe unauthorized behaviors, or determine the presence of prohibited items such as firearms or explosives. Effectively securing facility assets may also involve installation of additional physical barriers such as internal fences, security enclosures, additional access-control requirements, or special security procedures. Defensive measures used to secure facility assets often protect those assets by delaying or preventing the adversary from reaching or sabotaging the asset, or by physically protecting the asset from the effects of explosives, fire, or tampering.

Measures used to secure facility assets may be active, passive, or a combination of both. Active measures are either manually or automatically activated whereas passive measures are already in place and do not rely upon some initiating event.

To effectively secure facility assets against forced entry or sabotage, detection of the adversary generally should occur at a point where there is sufficient delay between the point of detection and the arrival of adequate response forces. Detection through monitoring may be achieved by direct human observation or by using a combination of technical security measures (e.g., alarm sensors, CCTV, thermal imagers, intelligent video) and human assessment of the situation to initiate the correct response.

Security Measures and Considerations for Securing Site Assets

Security Measures

Increasing reliance should be placed on physical and technical systems to provide additional protection for critical assets and any related chemicals of interest. Threat, typically related to the type of chemical of interest and sophistication of the adversary, defines the physical-security challenges of securing facility assets. Effective protective systems frequently integrate the following mutually supporting elements: physical protective measures, procedural security measures, and counteractions or measures to facilitate the response to terrorist attack.

Perimeter Barriers

Perimeter barriers provide both physical obstacles and psychological deterrents to unauthorized entry, delaying or preventing forced entry. Example barriers that could be implemented in support of RBPS 2 include, but are not limited to:

- Barriers to defeat/delay humans on foot (e.g., fences, gates)
- Barriers to defeat/deflect vehicles (e.g., jersey barriers, berms, bollards, planters)
- Natural or landscaping barriers (e.g., hedge rows, rocks, timber, water)
- Walls (e.g., brick, cinder block, poured concrete)

Perimeter barriers can be used in a variety of ways to restrict the area perimeter and increase overall facility security, including:

- Controlling vehicular and pedestrian access
- Providing channeling to facility entry-control points
- Delaying forced entry
- Protecting critical assets

Additional information on each of these types of barriers, including specific examples of each, can be found in Appendix C, along with things to consider when determining which, if any, perimeter barriers to implement.

Monitoring and Detection

Monitoring and detection equipment are key components of an effective perimeter security posture. Often, facilities will monitor for security events through a combination of human oversight and one or more electronic sensors or other intrusion detection system (IDS) components interfaced with electronic entry-control devices and alarm reporting displays. Typically, when a sensor or other IDS component identifies an event of interest, an alarm notifies security to assess the event either directly, by sending persons to the location of the event, or remotely by personnel evaluating sensor inputs and surveillance imagery.

There are many possible configurations of intrusion detection system (IDS) components that together satisfy the RBPS for securing and monitoring the facility perimeter. IDS for high-risk chemical facilities often use a combination of two or more of the following items:

- Fence-mounted, beam, or open area sensors (e.g., vibration detection sensors, video motion detection, infrared sensors, acoustic sensors)
- Remote surveillance (e.g., CCTV cameras, thermal images, IP cameras)
- Human-based monitoring via protective forces.

To increase the reliability of a monitoring system, an owner/operator may elect to deploy multiple interactive, redundant, or sophisticated sensors or counter-measures at high-risk locations with the understanding that increased reliability also extends to the functional capabilities of the data-transmission system.

An integrated technical perimeter security system should not only consider the sensors, remote surveillance, and human monitoring, but also the means of transmitting data gathered by the monitoring system, and a reporting process for monitoring, controlling, and displaying information on security events. When such electronic components are included in the perimeter monitoring system, the owner/operator may wish to locate alarm reporting devices and video monitors in a command and control center. Routine functions carried out in a control center may include selecting and assessing alarms; controlling video recording, playback, and display; checking the status of system components; changing sensor states; conducting some system self-tests; and controlling door locks.

Additional information on monitoring equipment, IDS elements, and command and control centers, can be found in Appendix C, along with things to consider when determining which, if any, sensors, remote surveillance, and protective forces to deploy.

Security Lighting

Security lighting can help to both deter attempts at penetrating a facility's perimeter and assist in the monitoring and detection of any such attempts. Inadequate lighting can make it more difficult to monitor a perimeter and detect attempts to breach the perimeter either directly through human protective forces, or through certain types of monitoring and intrusion detection systems, such as CCTVs. Due to the increased likelihood of detection based on appropriate security lighting, maintaining a well lit facility perimeter also can help deter adversaries from attempting to breach that perimeter.

A wide variety of different types of security lighting is available for implementation at facilities. When determining if security lighting is an appropriate part of a facility's security posture and what type of lighting to choose, a facility should consider such items as local weather conditions, available power sources, grounding, and interoperability with and support to other monitoring and detection systems, such as CCTVs. More detailed information on security considerations relevant to this RBPS can be found below.

Protective Forces

Protective forces are often used to enhance perimeter security and provide a means of deterrence, detection, delay, and response. Such forces can be proprietary or contracted, and can be armed or unarmed. Protective forces can be used in a variety of ways, including standing post at critical assets, monitoring critical assets using remote surveillance, or conducting roving patrols on a documented schedule that specifically includes identified targets, processes, or assets. Protective forces may be qualified to interdict adversaries themselves, or simply to deter and detect suspicious activities and to then call local law enforcement to provide an interdiction.

No matter how they are deployed, protective forces alone generally do not provide sufficient perimeter security. Accordingly, if a facility employs protective forces, they likely will need to be used in combination with one or more of the other measures listed above to provide an appropriate level of security to meet the Restrict Area Perimeter performance standard.

Security Considerations

Layered Security/Combining Barriers and Monitoring to Increase Delay

Completely adequate perimeter security is rarely achievable through the deployment of a single security barrier or monitoring system; rather an optimal security solution typically involves the use of multiple protective measures providing "layers of security." Layering of security measures can be achieved in many different manners, such as:

- Incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems with procedural security measures, such as procedures guiding how a security should respond to an incident)
- Using multiple lines of detection used to achieve protection-in-depth at critical assets
- Using complementary sensors with different means of detection (e.g., a CCTV and an intrusion detection system) to cover the same area.

A layered approach to perimeter security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

Securing Entire Perimeter vs. Securing Individual Asset

Depending on the size and location of the asset or assets driving a tier's risk, it may be more cost-effective to focus security directly on the asset(s) rather than the entire facility perimeter. For instance, if a facility is a large facility (e.g., covering 10 square miles) that has a single, relatively small Tier 1 asset (e.g., a single building or container), it likely would be significantly more cost-effective to apply Tier 1 level perimeter barriers solely around the perimeter of the Tier 1 asset rather than the entire facility. Accordingly, an owner/operator may wish to consider the benefits and costs related to completely enclosing a large facility within a single perimeter versus implementing multiple smaller restricted area perimeters.

Additional discussion on the pros and cons of securing an entire perimeter versus securing the individual high-risk assets contained therein is discussed in the Introduction. For performance objectives related to securing individual assets, an owner/operator should refer to RBPS 2 – Secure Site Assets.

Physical and Environmental Considerations

When determining the selection and layout of asset perimeter security components, a facility owner/operator should take into consideration the physical and environmental characteristics of the facility. Important *physical considerations* for evaluating the cost-effectiveness of perimeter countermeasures include:

- Perimeter length and convolution
- Terrain and urbanization
- Adjacent facilities and transportation corridors
- Approach angles and vehicle speeds
- Availability of supporting infrastructure
- Response capabilities and timelines

In addition to the physical considerations listed above, *environmental factors* also should be considered when making decisions regarding asset perimeter security, as certain environmental conditions can significantly affect sensor and lighting performance. For example, certain sensors or other IDS components that have near perfect detection capabilities during good weather might be subject to unacceptably high levels of false alarms during inclement weather (e.g., fog, rain, wind). Similarly, security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather. Accordingly, an owner/operator should consider the impact of environmental conditions when making determinations regarding security lighting and sensors or other IDS components.

Additional discussion on physical and environmental factors to take into consideration when making security decisions can be found in Appendix C.

Command and Control Considerations

Many security measures, such as intrusion detection systems or CCTV systems, consist of various hardware and software elements that can only be effectively operated or monitored by trained personnel, and owner/operators often will locate these functions in a command and control center. When designing security command and control centers, the facility owner/operator should consider merging security monitoring and reporting systems with other systems such as fire engineering reporting systems or process control systems. Technical merger of an active security system and a passive fire system may facilitate a common set of operational procedures (e.g., reporting, training, and emergency response), and prove a more cost-effective approach to overall facility safety and security management.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 4: RBPS Metrics – RBPS 2 – Secure Site Assets				
RBPS 2 – Secure Site Assets - Secure and monitor restricted areas or potentially critical targets within the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has additional vigorous barriers and systems to secure each restricted area and critical target, including a highly reliable system that continuously monitors each restricted area and critical target, and can demonstrate an extremely high probability that unauthorized adversary actions would be detected and access would be denied to restricted areas or critical targets, such as those containing chemicals of interest.	The facility secures and continuously monitors each restricted area and critical target and can demonstrate a high probability that unauthorized adversary actions towards restricted areas or critical targets, such as those containing chemicals of interest, would be detected.	The facility secures and regularly monitors each restricted area and critical target and can demonstrate a likelihood that unauthorized adversary actions towards restricted areas or critical targets, such as those containing chemicals of interest, would be detected.	The facility secures and periodically monitors each restricted area and critical target to detect unauthorized adversary actions towards restricted areas or critical targets, such as those containing chemicals of interest.

Table 4: RBPS Metrics – RBPS 2 – Secure Site Assets				
RBPS 2 – Secure Site Assets - Secure and monitor restricted areas or potentially critical targets within the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 2.1 – Asset Perimeter Barriers	To protect Tier 1 assets, the facility has an internal perimeter barrier, where feasible and consistent with critical operational and safety considerations, that severely restricts or delays any attempts by unauthorized persons to gain access to a restricted area or critical target, such as a chemical of interest. Such barriers could include a security fence or equivalent barrier that meets industrial consensus standards. A clearly-defined and well-secured facility perimeter, combined with high performance asset monitoring and strict administrative controls on asset access, can be an acceptable alternative to a secondary physical barrier.	N/A		
Metric 2.2 – Asset Vehicle Barriers	Vehicles would have a very low likelihood of accessing the target asset by force. To achieve this, a facility could, for example, use vehicle deterrence measures such as bollards, berms, landscaping, ditches, drainage swales, or buried concrete anchors retaining anti-vehicle cable wherever the perimeter is accessible to a vehicle.	Vehicles would have a low likelihood of accessing the target asset by force. To achieve this, a facility could, for example, use vehicle deterrence measures such as bollards, berms, landscaping, ditches, drainage swales, or buried concrete anchors retaining anti-vehicle cable wherever the perimeter is accessible to a vehicle.	N/A	
Metric 2.3 – Asset Standoff Distance	Sufficient vehicle standoff distance or alternative protective means are provided to ensure that vehicle-borne improvised explosive devices will not cause a breach of containment resulting in an uncontrolled release of a chemical of interest from the nearest point of attack.		N/A	
Metric 2.4 – Monitoring and Surveillance	A combination of highly reliable technical security devices (e.g., special access controls, sensors, video), security patrols, and other monitoring systems are used to protect and continuously	Reliable technical security devices (e.g., special access controls, sensors, video), security personnel, and/or monitoring systems are used to protect and continuously monitor critical asset	Reliable technical security devices (e.g., special access controls, sensors, video), security personnel, and/or monitoring systems are used to protect and monitor critical asset locations	Technical security devices (e.g., special access controls, sensors, video), security personnel, and/or monitoring systems are used to protect and monitor and critical asset locations

Table 4: RBPS Metrics – RBPS 2 – Secure Site Assets				
RBPS 2 – Secure Site Assets - Secure and monitor restricted areas or potentially critical targets within the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	monitor restricted areas or critical asset locations (including COI loading and unloading areas, critical valves, pipelines, manifolds, control rooms, and storage facilities) to detect attempts to gain unauthorized access, tampering, attempted sabotage, or theft or unauthorized removal of critical assets such as chemicals of interest. To achieve this, a facility could, for example, use a combination of measures such as: • Posted security personnel or frequent security patrols. • An integrated, multi-sensor system that provides intrusion detection and video surveillance around 100% of the perimeter of the critical assets, has emergency back up power and/or an equivalent written contingency procedure, and whose images are continuously monitored by a dedicated persons, software, or other detection methods used in conjunction with the system. • General area as well as access portal (face view) CCTV surveillance at all gates.	locations (including COI loading and unloading areas, critical valves, pipelines, manifolds, control rooms, and storage facilities) to detect attempts to gain unauthorized access, tampering, attempted sabotage, or theft or unauthorized removal of critical assets such as chemicals of interest. To achieve this, a facility could, for example, use a combination of measures such as: • Frequent security patrols. • An integrated monitoring system that provides intrusion detection and video surveillance around designated COI or other target assets, has emergency back up power and/or an equivalent written contingency procedure, and whose images are continuously monitored by a dedicated persons, software, or other detection methods used in conjunction with the system.	(including COI loading and unloading areas, critical valves, pipelines, manifolds, control rooms, and storage facilities) to detect attempts to gain unauthorized access, tampering, attempted sabotage, or theft or unauthorized removal of critical assets such as chemicals of interest. To achieve this, a facility could, for example, use a combination of measure such as: • Regular security patrols. • An integrated monitoring system that provides intrusion detection and video surveillance around designated COI or other target assets and has emergency back up power and/or an equivalent written contingency procedure.	(including COI loading and unloading areas) to detect attempts to gain unauthorized access, tampering, attempted sabotage, or theft or unauthorized removal of critical assets such as chemicals of interest. To achieve this, a facility could, for example, use measures such as periodic security patrols or an integrated monitoring system that provides intrusion detection and video surveillance around designated COI or other target assets and has emergency back up power and/or an equivalent written contingency procedure.

RBPS 3 – Screen and Control Access

RBPS 3 - Screen and Control Access - Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including:
(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures.

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 3 – Screen and Control Access is focused on the identification, screening, and/or inspection of individuals and vehicles as they enter and exit the facility. Through identification, screening, and inspection, a facility is better able to prevent unauthorized access to the facility and more likely to deter and detect unauthorized introduction or removal of substances and devices that may cause a dangerous chemical reaction, explosion, or hazardous release.

Security Measures and Considerations for Screening and Controlling Assets

Security Measures

A variety of different types of measures may be used in conjunction to address RBPS 3 – Screen and Control Access. These include screening measures (e.g., personnel identification, hand-carried items inspections, vehicle identification, and vehicle inspections), control point measures (e.g., measures to control vehicular approach and denial); and parking security measures.

Personnel Identification

A primary component of successfully screening and controlling access is knowing who is allowed on-site. Personnel identification measures help a facility quickly determine whether or not an individual is permitted facility access, and certain identification measures can help both security officers and other employees quickly know whether or not an individual is authorized for facility access. Examples of personnel identification measures may include:

- Conducting checks of government issued photo IDs prior to permitting facility access
- Providing company issued photo IDs to individuals permitted access to the facility or restricted areas of the facility, identifying:
  - Employees
  - Regular contractors
  - Temporary contractors
  - Visitors
- Providing facility-specific photo IDs to individuals permitted access to the facility or to restricted areas of the facility, identifying:
  - Employees
  - Regular contractors
  - Temporary contractors
  - Visitors

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Screen and Control Access performance standards, a facility might consider the following potential attack scenarios:

- Assault Team
- Sabotage
- Stand-Off
- Theft/Diversion
- VBIED

Depending on the level of security desired, a company may want to issue photo IDs (company or facility-specific) that are linked with electronic access control systems such as proximity ID readers or swipe access controls for an added layer of security. Electronic access control systems can be tailored to specific locations within a facility, thus providing the ability to limit access to restricted areas to authorized individuals. They also have the additional benefit of maintaining a record regarding who has accessed what areas.

A personnel identification system is most effective when used in conjunction with the performance of background checks and other personnel surety measures. Such measures are the focus of RBPS 12 – Personnel Surety.

Hand-carried Items Inspection

A second common element of many good screening programs is the inspection of items brought into the facility or restricted areas of the facility, whether brought in by employees, contractors, or visitors. Among other things, inspections may include:

- Visual inspections
- X-ray inspections
- Use of metal detectors
- Use of ionic explosives detection equipment
- Use of trained explosive detection canines

The type of inspection measures implemented, the thoroughness of inspections, and the frequency of inspections may vary based on a variety of factors, including the facility's tier (e.g., more vigorous and frequent measures may be suitable for higher tiers) and who is being inspected (e.g., more frequent and thorough inspections may be desired for visitors than for employees).

Vehicle Identification and Inspection

Another element of a comprehensive screening program is a vehicle identification and inspection program.

Vehicle identification measures can include using a company or facility-issued vehicle ID system (e.g., providing authorized vehicles with stickers or placards), using only known shippers and/or delivery companies, and requiring authorized bills of lading for access to the facility. These types of measures can help satisfy the standards established for RBPS 5 – Shipping, Receipt, and Storage, and are complemented by other measures recommended for RBPS 5 compliance.

Vehicle inspection measures that can be helpful in meeting the screening and access control standards include:

- Visual inspections
- Use of trained explosive detection canines
- Under/over vehicle inspection systems
- Cargo inspection systems

Much like hand-carried item inspections, the type of vehicle inspection measures implemented, the thoroughness of inspections, and the frequency of inspections may vary based on a variety of factors, including the facility's tier (e.g., more vigorous and frequent inspections may be suitable for higher tiers) and whose vehicle is being inspected (e.g., more frequent and thorough inspections may be desired for visitors or unscheduled delivery trucks than for employees or regularly scheduled deliveries).

Control Point Measures

Control point measures are measures used to help control vehicular access to a facility, by calming traffic as it approaches the facility, providing an opportunity for vehicle identification to occur, and by denying facility access to unauthorized vehicles. Control point measures may include:

- Aligning roads in a manner to calm traffic (e.g., circles, serpentine roads)
- Bollards, barriers, K-Rails, etc. to cause serpentine traffic flow
- Speed bumps or tables
- Gates
- Identification points and rejection points prior to facility access

More information on these types of measures can be found in Appendix C.

Parking Security Measures

By limiting or managing parking on-site, a facility can help minimize ease of access to critical assets located inside the facility's perimeter. While completely prohibiting on-site parking is one option, less extreme measures are available, such as limiting on-site parking to certain vehicle classes—e.g., only "corporate" vehicles allowed on-site or only full-time employee vehicles allowed on-site (i.e., no visitor or contractor parking within the facility perimeter). Another option is to allow parking on-site, but locate it a significant distance away from the critical assets, and prevent means of vehicular egress to the critical assets.

Security Considerations

Layered Security/Combining Barriers and Monitoring to Increase Delay

No matter the size of the individual asset being secured, completely adequate security likely will not be achievable through the deployment of a single protective measure; rather an optimal security solution typically involves the use of multiple protective measures providing "layers of security." Layering of security measures can be achieved in many different manners, such as:

- Incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems with procedural security measures, such as procedures guiding how a security should respond to an incident)
- Using multiple lines of detection used to achieve protection-in-depth at critical assets
- Using complementary sensors with different means of detection (e.g., a CCTV and an intrusion detection system) to cover the same area.

A layered approach to asset security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

Physical and Environmental Considerations

When determining the selection and layout of asset security components, a facility owner/operator should take into consideration the physical and environmental characteristics surrounding the asset. Important *physical considerations* for evaluating the cost-effectiveness of countermeasures include:

- Asset size and asset perimeter length and convolution
- Terrain and urbanization
- Adjacent facilities and transportation corridors
- Approach angles and vehicle speeds
- Availability of supporting infrastructure

In addition to the physical considerations listed above, *environmental factors* also should be considered when making decisions regarding asset security, as certain environmental conditions can significantly affect sensor and lighting performance. For example, certain sensors or other IDS components that have near perfect detection capabilities during good weather might be subject to unacceptably high levels of false alarms during inclement weather (e.g., fog, rain, wind). Similarly, security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather. Accordingly, an owner/operator should consider the impact of environmental conditions when making determinations regarding security lighting and sensors or other IDS components.

Additional discussion on physical and environmental factors to take into consideration when making security decisions can be found in Appendix C.

Command and Control Considerations

Many asset security measures, such as intrusion detection systems or CCTV systems, consist of various hardware and software elements that can only be effectively operated or monitored by trained personnel, and owner/operators often will locate these functions in a command and control center. When designing command and control centers, owner/operators should consider merging security monitoring and reporting systems with other systems such as fire engineering reporting systems or process control. Technical merger of an active security system and a passive fire system may facilitate a common set of operational procedures (e.g., reporting, training, and emergency response), and prove a more cost-effective approach to overall facility safety and security management.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 5: RBPS Metrics – RBPS 3 – Screen and Control Access

RBPS 3 – Screen and Control Access - Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including:
(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures.

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	The facility employs a strict process for controlling access to the facility and screening all persons and vehicles seeking access to restricted-areas. The process deters the unauthorized introduction of dangerous substances and devices to the facility, and, via a near real-time updated system, checks the identification of facility personnel and other persons seeking access to the facility. The facility can demonstrate an extremely high probability of detecting and preventing fraudulent entry and has a system to report such attempts to law enforcement.	The facility employs a process for controlling access to the facility and screening a high percentage of selected persons and vehicles seeking access to restricted-areas. The process deters the unauthorized introduction of dangerous substances and devices to the facility, and, via a frequently updated system, checks the identification of facility personnel and other persons seeking access to the facility. The facility can demonstrate a high probability of detecting and preventing fraudulent entry and has a system to report such attempts to law enforcement.	The facility employs a process for controlling access to the facility and screening selected persons and vehicles seeking access to restricted-areas. The process deters the unauthorized introduction of dangerous substances and devices to the facility, and, via a routinely updated system, checks the identification of facility personnel and other persons seeking access to the facility. The facility can demonstrate a likelihood of detecting and preventing fraudulent entry and has a system to report such attempts to law enforcement.	The facility employs a process for controlling access to the facility and screening selected persons and vehicles seeking access to restricted-areas. The process deters the unauthorized introduction of dangerous substances and devices to the facility, and checks the identification of facility personnel and other persons seeking access to the facility. The facility has the capability to detect some attempts at fraudulent entry and has a system to report such attempts to law enforcement.
Metric 3.1 – Access Point Controls	The facility has a comprehensive access control system that can demonstrate an extremely high reliability to thwart adversary attempts to gain unauthorized access. To achieve this, a facility could, for example, use a combination of measures, such as the following: • A system providing for the verification of the authorization for access by a photo identification card or biometrics. • Access points are manned by security personnel when open for use, and are either manned or continuously monitored at all other times.	The facility has an access control system that can demonstrate a high reliability to thwart adversary attempts to gain unauthorized access. To achieve this, a facility could, for example, use a combination of measures, such as following: • A system providing for the verification of the authorization for access by a photo identification card or biometrics. • Access points are manned by security personnel when open for use, and are either manned or continuously monitored at all other times. • Gates and anti-passback	The facility has an access control system that reliably thwarts adversary attempts to gain unauthorized access. To achieve this, a facility could, for example, use a combination of measures, such as the following: • A system providing for the verification of the authorization for access by a photo identification card or electronic key access. • Access points are either manned by security personnel or are closed and monitored. • Gates and anti-passback devices (e.g., turnstiles) activated by an electronic access system using	The facility has a system to verify the identity of individuals seeking entry to restricted areas to control unauthorized access, such as use of a photo identification card or electronic key access. Facility access points are either manned or closed and monitored.

Table 5: RBPS Metrics – RBPS 3 – Screen and Control Access				
RBPS 3 – Screen and Control Access - Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including: (i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and (ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	• Gates and anti-passback devices (e.g., turnstiles) activated by an electronic access system using badges for vehicle and personnel entrances for both the outer perimeter and internal restricted areas. • One or more separate access gates for contractor personnel. • Access control systems that are programmable to allow multi-level access.	devices (e.g., turnstiles) activated by an electronic access system using badges for vehicle and personnel entrances for both the outer perimeter and internal restricted areas. • Access control systems that are programmable to allow multi-level access.	badges for vehicle and personnel entrances for both the outer perimeter and internal restricted areas.	

Table 5: RBPS Metrics – RBPS 3 – Screen and Control Access

RBPS 3 – Screen and Control Access - Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including:
(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures.

	Tier 1	Tier 2	Tier 3	Tier 4
Metric 3.2 – Identity Verification Systems	Unauthorized persons would be highly unlikely to gain unauthorized access due to the vigorousness of identity verification systems. To achieve this, a facility could, for example, use a combination of measures, such as the following: • All employees and other selected persons (e.g., resident contractors, transport drivers) are issued tamper resistant ID badges with, at a minimum, the individual's name and photo, which are worn in a visible position when on-site. • All other personnel are documented, issued a temporary badge, and escorted while in restricted areas, and escorted or continuously monitored elsewhere on-site. • Unknown vehicles remain outside the facility perimeter or in a secured area while they and their occupants are being vetted. • All unescorted personnel (e.g., employees, regular contractors, and transport drivers) are issued electronic photo ID badges integrated with the facility access control system.	Unauthorized persons would be unlikely to gain unauthorized access due to the vigorousness of identity verification systems. To achieve this, a facility could, for example, use a combination of measures, such as the following: • All employees and other selected persons (e.g., resident contractors, transport drivers) are issued tamper resistant ID badges with, at a minimum, the individual's name and photo, which are worn in a visible position when on-site. • All other personnel are documented, issued a temporary badge, and escorted while in restricted areas, and escorted or continuously monitored elsewhere on-site. • Unknown vehicles remain outside the facility perimeter or in a secured area while they and their occupants are being vetted. • All unescorted personnel (e.g., employees, regular contractors, and transport drivers) are issued electronic photo ID badges integrated with the facility access control system.	The facility has access control systems that provide for reasonable identity verification, such as the issuing of tamper resistant ID badges to all facility employees, and the provision of visitor badges to, and escorting or monitoring of, all individuals without permanent ID badges.	

Table 5: RBPS Metrics – RBPS 3 – Screen and Control Access				
RBPS 3 - Screen and Control Access - Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including: (i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and (ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 3.3 – On-site Parking	Parking on-site is minimized and vehicular access to restricted areas is restricted (e.g., only company vehicles are allowed on-site, no personally owned vehicles may park on-site, and no delivery vehicles are allowed on-site without an escort).	Parking on-site is minimized and vehicular access to restricted areas is restricted (e.g., company vehicles and a very limited number of personally owned employee or contractor vehicles are authorized to park on-site, no visitors may park on-site, and delivery vehicles are escorted in restricted areas).	Authorized employee, contractor, and visitor vehicles parking on-site are kept to a minimum and some authorized delivery vehicles may have unescorted facility access.	N/A
Metric 3.4 – Screening and Inspections	The facility has a comprehensive screening system that extremely reliably deters the unauthorized introduction of dangerous substances to the facility. A typical facility may use various means, such as the following, to achieve this standard: • The facility has the ability to inspect all vehicles and all of the items carried by individuals seeking access to the facility, and, under normal operating procedures, performs random, rigorous inspections of at least 30% of all vehicles and hand-carried items both inbound and, for where theft/diversion or sabotage assets are located, outbound. • Inspections of individuals themselves are performed when the situation warrants. • Trucks and rail cars are inspected upon entering the facility and prior to loading.	The facility has a screening system that reliably deters the unauthorized introduction of dangerous substances to the facility. A typical facility may use various means, such as the following, to achieve this standard: • The facility has the ability to inspect all vehicles and all of the items carried by individuals seeking access to the facility, and, under normal operating procedures, performs random, rigorous inspections of at least 15% of all vehicles and hand-carried items. • Inspections of individuals themselves are performed when the situation warrants. • A percentage of trucks and rail cars are subject to random inspection upon entering the facility and prior to loading.	The facility has a screening system that reasonably deters the unauthorized introduction of dangerous substances to the facility. A typical facility may use various means, such as the following, to achieve this standard: • The facility has the ability to inspect all vehicles and all of the items carried by individuals seeking access to the facility, and, under normal operating procedures, performs random, rigorous inspections of at least 5% of all vehicles and hand-carried items. • Inspections of individuals themselves are performed when the situation warrants. • A percentage of trucks and rail cars are subject to random inspection upon entering the facility and prior to loading.	The facility has a screening system that reasonably deters the unauthorized introduction of dangerous substances to the facility, and performs inspections of vehicles, individuals, and hand-carried items when the situation warrants.

RBPS 4 – Deter, Detect, and Delay

RBPS 4 – Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;

(iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and

(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

Adequate protection depends upon the overlapping principles of deterrence, detection, and delay combined with an effective response to unauthorized acts or individuals.

Deterrence refers to the ability to cause a potential attacker to perceive that the risk of failure is greater than that which they find acceptable, resulting in a determination that an attack is not worth the risk. Thus, deterrence measures are focused not on detecting or stopping an attack once in progress, but rather on convincing an adversary not to attack in the first place. The value of deterrence measures varies with the sophistication of the adversary, target attractiveness, and the difficulty of the attack.

Detection refers to the ability to identify potential attacks or precursors to an attack, and to communicate that information as appropriate. Detection measures typically include surveillance and other types of monitoring similar or identical to those applied in support of RBPS 1 – Restrict Area Perimeter. For a protective system to prevail, detection needs to occur prior to an attack (i.e., in the attack planning stages), or early enough in the attack where there is sufficient delay between the point of detection and the successful conclusion of the attack for the arrival of adequate response forces to thwart the attempt.

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Deter, Detect, and Delay performance standards, a facility might consider the following potential attack scenarios:

- Assault Team
- Maritime
- Sabotage
- Stand-Off
- Theft/Diversion
- VBIED

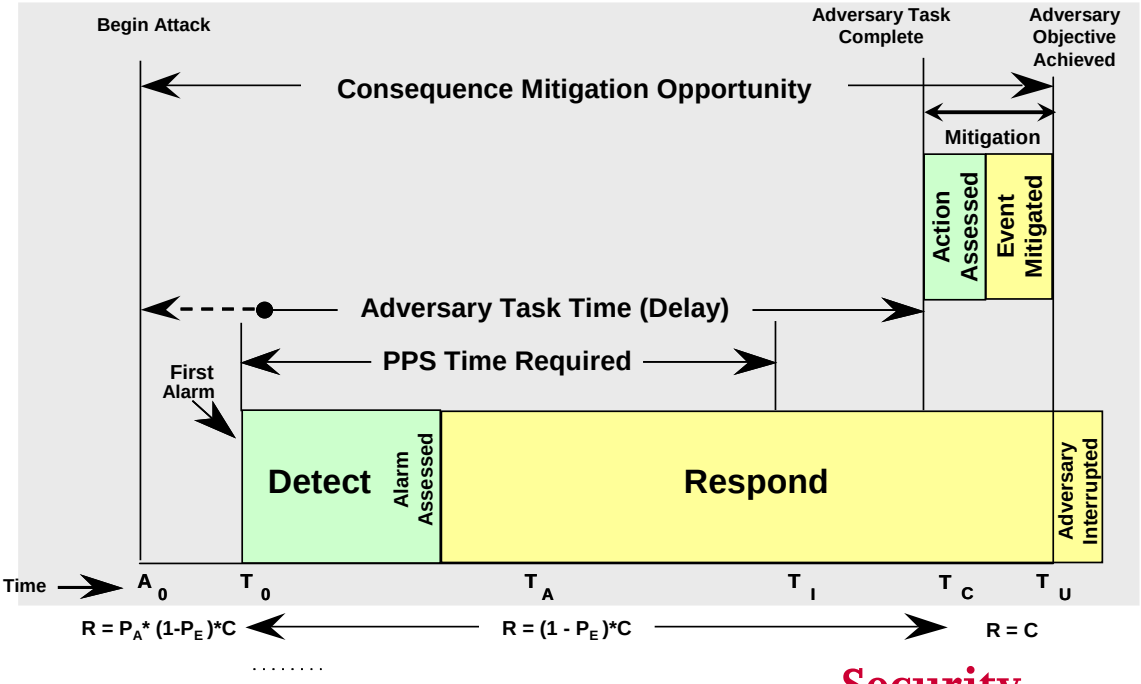
Delay refers to the ability to slow down an adversary's progress sufficiently to allow adequate protective forces to respond. Delay is often achieved through defensive measures used to protect critical assets, hardened targets, or response force engagement that prevents the adversary from reaching the target asset in an expeditious manner.

RBPS 4 provides standards for deterrence, detection, and delay for each tier. The expectation is that covered facilities, to varying degrees, will be able to deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including:

- Measures to deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
- Measures to deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
- Detecting attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
- Delaying an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.

Figure 2 illustrates in a timeline the concept of integrating adequate detection and mitigation (response). Response could be a range of activities such as isolating a process, shutting down a critical operation, locking of doors, activating alarms, interdicting through an on-site guard force, activating a safety system to limit the effects of an intentional release, or evacuation or shelter in place.

Figure 2 - Concept of Integrating Adequate Detection and Mitigation (Source: Sandia)



Security Measures and Considerations to Deter, Detect, and Delay

There are many different types of security measures which can be effectively used to deter, detect, and/or delay an adversary. These include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. Often, a single measure can accomplish more than one of the deter, detect, delay principles.

Security Measures

Perimeter Barriers

Perimeter barriers serve to deter an adversary from attempting to attack and help delay (or entirely prevent) unauthorized entry. Sample barriers that have deterrence and or delaying affects include, but are not limited to:

- Human barriers (e.g., fences, gates)
- Vehicle barriers (e.g., jersey barriers, berms, bollards, planters)
- Natural or landscaping barriers (e.g., hedge rows, rocks, timber, water)
- Walls (e.g., brick, cinder block, poured concrete)

Additional information on each of these types of barriers, including specific examples of each, can be found in Appendix C, along with things to consider when determining which, if any, perimeter barriers to implement. More detailed information on security considerations relevant to this RBPS can be found below.

Monitoring and Detection Systems

Monitoring and detection equipment are key components of any effective deterrence and detection strategy. Often, facilities will monitor for security events through a combination of human oversight and one or more electronic sensors or other intrusion detection system (IDS) components interfaced with electronic entry-control devices and alarm reporting displays. Typically, when a sensor or other IDS component identifies an event of interest, an alarm notifies security, which then will assess the event either directly by sending persons to the location of the event or remotely by personnel evaluating sensor inputs and surveillance imagery.

There are many possible configurations of intrusion detection system (IDS) components that serve to deter and detect adversaries. These include:

- Fence-mounted, beam, or open area sensors (e.g., vibration detection sensors, video motion detection, infrared sensors, acoustic sensors)
- Remote surveillance (e.g., CCTV cameras, thermal images, IP cameras)
- Human-based monitoring via protective forces (further details on protective forces can be found below).

Additional information on each of these IDS elements, including specific examples of each, can be found in Appendix C, along with things to consider when determining which, if any, sensors, remote surveillance, and protective forces to deploy. More detailed information on security considerations relevant to this RBPS can be found below.

Security Lighting

Security lighting both helps to deter attacks on a facility and detect any such attempts. Inadequate lighting can make it more difficult to monitor a perimeter and detect attempts to breach the perimeter either directly through human protective forces, or through certain types of monitoring and intrusion detection systems, such as CCTVs. Due to the increased likelihood of detection based on appropriate security lighting, maintaining a well lit facility perimeter also can help deter adversaries from attempting to breach that perimeter.

A wide variety of different types of security lighting is available for implementation at facilities. When determining if security lighting is an appropriate part of a facility's security posture and what type of lighting to choose, a facility should consider such items as local weather conditions, available power sources, grounding, and interoperability with and support to other monitoring and detection systems, such as CCTVs. More detailed information on security considerations relevant to this RBPS can be found below.

Protective Forces

Protective forces are often used to enhance perimeter security and provide a means of deterrence, detection, delay, and response. Such forces can be proprietary or contracted, and can be armed or

unarmed. They may be qualified to interdict adversaries themselves, or simply to deter and detect suspicious activities and to then call local law enforcement to provide an interdiction.

Security Considerations

Layered Security/Combining Barriers and Monitoring to Increase Delay

Complete deterrence, detection and delay is not achievable through the deployment of a single security barrier or monitoring system; rather an optimal security solution typically involves the use of multiple protective measures providing "layers of security." Layering of security measures can be achieved in many different manners, such as:

- Incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems with procedural security measures, such as procedures guiding how a security should respond to an incident)
- Using multiple lines of detection used to achieve protection-in-depth at critical assets
- Using complementary sensors with different means of detection (e.g., a CCTV and an intrusion detection system) to cover the same area.

A layered approach to security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost. More information on layered approaches to security can be found in Appendix C.

Securing Entire Perimeter vs. Securing Individual Asset

Depending on the size and location of the asset or assets driving a tier's risk, it may be more cost-effective to focus deterrence, detection, and delay efforts towards the asset(s) rather than the entire perimeter. For instance, if a facility is a large facility (e.g., covering 10 square miles) that has a single, relatively small Tier 1 asset (e.g., a single building or container), it likely would be significantly more cost-effective to apply Tier 1 level perimeter barriers solely around the perimeter of the Tier 1 asset rather than the entire facility. Accordingly, an owner/operator may wish to consider the benefits and costs related to completely enclosing a large facility within a single perimeter versus implementing multiple smaller restricted area perimeters.

Additional discussion on the pros and cons of securing an entire perimeter versus securing the individual high-risk assets contained therein is discussed in the Introduction. For performance objectives related to securing individual assets, an owner/operator should refer to RBPS 2 – Secure Site Assets.

Physical and Environmental Considerations

When determining the selection and layout of deterrence, detection, and delay components, a facility owner/operator should take into consideration the physical and environmental characteristics of his or her facility. Important *physical considerations* for evaluating the cost-effectiveness of countermeasures include:

- Perimeter length and convolution
- Terrain and urbanization
- Adjacent facilities and transportation corridors
- Approach angles and vehicle speeds
- Availability of supporting infrastructure

In addition to the physical considerations listed above, *environmental factors* also should be considered when making decisions regarding deterrence, detection, and delay, as certain environmental conditions can significantly affect sensor and lighting performance. For example, certain sensors or other IDS components that have near perfect detection capabilities during good weather might be subject to unacceptably high levels of false alarms during inclement weather (e.g., fog, rain, wind). Similarly, security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather. Accordingly, an owner/operator should consider the impact of environmental conditions when making determinations regarding security lighting and sensors or other IDS components.

Additional discussion on physical and environmental factors to take into considerations when making security decisions can be found in Appendix C.

Command and Control Considerations

Many security measures, such as intrusion detection systems or CCTV systems, consist of various hardware and software elements that can only be effectively operated or monitored by trained personnel, and owner/operators often will locate these functions in a command and control center. When designing command and control centers, owner/operators should consider merging security monitoring and reporting systems with other systems, such as fire engineering reporting systems or process control. Technical merger of an active security system and a passive fire system may facilitate a common set of operational procedures (e.g., reporting, training, and emergency response) and prove a more cost-effective approach to overall facility safety and security management.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 6: RBPS Metrics – RBPS 4 – Deter, Detect, and Delay

RBPS 4 - Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:
(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
(iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	Through a series of protective security layers incorporating strong security measures, the facility has a very high likelihood of deterring, detecting, and delaying all adversaries to a degree sufficient to allow response to thwart the adversary action before it achieves mission success. This includes a highly reliable ability to deter penetration by an unauthorized vehicle, deter vehicle access to restricted areas, and deter vehicles presenting a hazard to potentially critical targets.	Through the use of security measures, the facility can deter, detect, and delay most adversaries to a degree sufficient to allow response to thwart the adversary action before it achieves mission success. This includes a reliable ability to deter penetration by an unauthorized vehicle, deter vehicle access to restricted areas, and deter vehicles presenting a hazard to potentially critical targets.	The facility can demonstrate a reasonable ability to deter, detect, and delay adversaries allowing appropriate response, including a reasonable ability to deter penetration by an unauthorized vehicle, deter vehicle access to restricted areas, and deter vehicles presenting a hazard to potentially critical targets.	The facility can demonstrate some ability to deter, detect, and delay adversaries, including some ability to deter penetration by an unauthorized vehicle, deter vehicle access to restricted areas, and deter vehicles presenting a hazard to potentially critical targets.
Metric 4.1 – Deterrence and Delay General	Through a combination of on-site security, barriers and barricades, hardened targets, and well-coordinated response planning, the facility has a very high likelihood of deterring an attack and/or delaying an attack for a sufficient period of time to allow appropriate response.	Through a combination of on-site security, barriers and barricades, hardened targets, and well-coordinated response planning, the facility has a high likelihood of deterring an attack and/or delaying an attack for a sufficient period of time to allow appropriate response.	Through a combination of on-site security, barriers and barricades, hardened targets, and well-coordinated response planning, the facility has some ability to deter and/or delay an attack allowing appropriate response.	The facility has some ability to deter and/or delay an attack allowing appropriate response through well-coordinated response planning.

Table 6: RBPS Metrics – RBPS 4 – Deter, Detect, and Delay				
RBPS 4 - Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to: (i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets; (ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets; (iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and (iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 4.2 – Deterrence and Delay Vehicle Barriers	The facility has highly reliable measures (e.g., DOS K8 or higher equivalent crash-rated anti-vehicle barrier) that deter vehicles from penetrating the facility perimeter, and make it highly unlikely that a vehicle could gain access by force or otherwise present a hazard to potentially critical targets. Desired barrier rating can vary based on maximum attainable vehicle speed at the barrier.	The facility has reliable measures (e.g., DOS K8 or equivalent crash-rated anti-vehicle barrier) that deter vehicles from penetrating the facility perimeter, and make it unlikely that a vehicle could gain access by force or otherwise present a hazard to potentially critical targets. Desired barrier rating can vary based on maximum attainable vehicle speed at the barrier.	The facility has measures (e.g., DOS K4 or equivalent crash-rated anti-vehicle barrier) that deter vehicles from penetrating the facility perimeter, and make it difficult for most vehicles to breach the control point by force or otherwise present a hazard to potentially critical targets. Desired barrier rating can vary based on maximum attainable vehicle speed at the barrier.	The facility has some measures (e.g., active or passive barriers) that deter vehicles from accessing the facility without authorization.

Table 6: RBPS Metrics – RBPS 4 – Deter, Detect, and Delay

RBPS 4 - Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:
(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
(iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.

	Tier 1	Tier 2	Tier 3	Tier 4
Metric 4.3 – Detection Monitoring and Surveillance	The facility has an extremely reliable perimeter monitoring system which continuously monitors the entire length of the facility perimeter, allows for the identification and evaluation of an intrusion in real time, and provides notification of intrusion to a continuously manned location. In the context of this metric, "real time" means that an adverse act virtually always is detected and reported to responders at the time of occurrence. "Extremely reliable" means that the monitoring system is operable during all anticipated conditions, including complete darkness, twilight, inclement weather, and loss of power; with monitoring system components designed, laid-out, and constructed to avoid common cause/dependent failures and provide redundant signal processing equipment where digital signal processing is used. To achieve this, a facility could, for example, use an integrated, multi-sensor system that: • Provides intrusion detection and video surveillance around 100% of the perimeter. • Whose images or other output are continuously monitored by a dedicated person, software, or other detection methods used in conjunction with the system. • Has emergency back up power and/or an equivalent written contingency procedure.	The facility has a very reliable perimeter monitoring system which continuously monitors the entire length of the facility perimeter, allows for the identification and evaluation of an intrusion in real time, and provides notification of intrusion to a continuously monitored location. In the context of this metric, "real time" means that an adverse act most likely is detected and reported to responders at the time of occurrence. "Very reliable" means that the monitoring system is operable during ambient light, inclement weather, and fluctuating power conditions; with monitoring system components designed, laid-out, and constructed so as to avoid common cause/dependent failures and provide redundant signal processing equipment where digital signal processing is used. To achieve this, a facility typically could, for example, use an integrated monitoring system that: • Provides intrusion detection and video surveillance around designated COI target assets that do not have passive vehicle barriers. • Whose images or other output are continuously monitored by a dedicated person, software, or other detection methods used in conjunction with the system.	The facility has a reliable perimeter monitoring system that allows for the identification of the presence of an intrusion in real time for the area(s) containing the target asset(s). In the context of this metric, "real time" means that an adverse act likely is detected and reported to responders in a timely manner. "Reliable" means that the monitoring system is be operable during ambient light conditions. To achieve this, a facility typically could, for example, use an integrated monitoring system that: • Provides intrusion detection and video surveillance around designated COI target assets. • Has emergency back up power and/or an equivalent written contingency procedure.	The facility has a monitoring system that allows for the identification of the presence of an intrusion in the area(s) containing the target asset(s). To achieve this, a facility typically will use security patrols of the facility or an integrated monitoring system that provides intrusion detection and video surveillance around designated COI target assets, is fully operable during all lighting conditions, and has emergency back up power and/or an equivalent written contingency procedure.

Table 6: RBPS Metrics – RBPS 4 – Deter, Detect, and Delay				
RBPS 4 - Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to: (i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets; (ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets; (iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and (iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	• General area as well as access portal (face view) CCTV surveillance at all gates.	• Has emergency back up power and/or an equivalent written contingency procedure.		
Metric 4.4 – Detection Security Operations Centers	The facility has a very high likelihood of detecting attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers or barricades. To achieve this level of detection, a facility typically maintains a facility-wide intrusion detection system that is continually monitored from a Security Operations Center, and has an adequate backup capability.	The facility has a high likelihood of detecting attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers or barricades. To achieve this level of detection, a facility typically maintains a facility-wide intrusion detection system that is continually monitored from a Security Operations Center.	The facility has some ability to detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers or barricades.	The facility has some ability to detect attacks at early stages.

Table 6: RBPS Metrics – RBPS 4 – Deter, Detect, and Delay				
RBPS 4 - Deter, Detect, and Delay - Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to: (i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets; (ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets; (iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and (iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 4.5 – Interdiction by Security Forces or Other Means	The facility is extremely likely to be able to detect and initiate a response to armed intruders resulting in the intruders being interdicted before they reach a COI target asset or other potentially critical target. This capability may be achieved by a facility security force, sufficient delay tactics to allow local law enforcement to respond before the adversary achieves mission success, standoff distances (for VBIEDs), process controls or systems that rapidly render the designated COI target asset(s) or other potentially critical target non-hazardous even if a breach of containment were to occur (e.g., a rapid chemical neutralization system), or other equivalent measures. If security forces are used, they may be contract or proprietary, mobile or posted, armed or unarmed, or a combination thereof.	The facility is likely to be able to detect and initiate a response to armed intruders resulting in the intruders being interdicted before they reach a COI target asset or other potentially critical target. This capability may be achieved by a facility security force, sufficient delay tactics to allow local law enforcement to respond before the adversary achieves mission success, standoff distances (for VBIEDs), process controls or systems that rapidly render the designated COI target asset(s) or other potentially critical target non-hazardous even if a breach of containment were to occur (e.g., a rapid chemical neutralization system), or other equivalent measures. If security forces are used, they may be contract or proprietary, mobile or posted, armed or unarmed, or a combination thereof.	The facility has some ability to detect and initiate a response to armed intruders resulting in the intruders being interdicted before they reach a COI target asset or other potentially critical target. This capability may be achieved by a facility security force, sufficient delay tactics to allow local law enforcement to respond before the adversary achieves mission success, standoff distances (for VBIEDs), process controls or systems that rapidly render the designated COI target or other potentially critical target non-hazardous even if a breach of containment were to occur (e.g., a rapid chemical neutralization system), or other equivalent measures. If security forces are used, they may be contract or proprietary, mobile or posted, armed or unarmed, or a combination thereof.	

RBPS 5 – Shipping, Receipt, and Storage

RBPS 5 – Shipping, Receipt, and Storage - Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 5 – Shipping, Receipt, and Storage performance standards are designed to help a facility minimize the risk of theft or diversion of any of its hazardous materials (e.g., chemicals of interest). In addition, improved inventory control and control of transportation containers on-site helps to prevent tampering or sabotage, and decreases the likelihood that a foreign substance could be introduced into feedstock, incidental chemicals, or products leaving the facility that could later interact with the chemical of interest or other hazardous material to cause a harmful reaction on- or off-site. Good shipping, receipt and storage practices typically include maintaining all transportation containers used for storage not incident to transportation, including transportation containers connected to equipment at a facility for loading or unloading and transportation containers detached from the motive power (e.g., a locomotive, truck/tractor) that delivered the container to the facility, inside the facility's security perimeter and under the security control of the facility.

Security Measures and Considerations for Shipping, Receipt, and Storage

Security Measures

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Shipping, Receipt, and Storage performance standards, a facility might consider the following potential attack scenarios:

- Assault Team
- Sabotage
- Stand-Off
- Theft/Diversion
- VBIED

Product Stewardship

Product stewardship is a term used to describe a product-centered approach to protection of hazardous materials, such as chemicals of interest, calling for manufacturers, retailers, and consumers to share responsibility for reducing the potential for theft, contamination, or misuse of toxic or flammable chemicals. Voluntary product stewardship activities have been taking place within the chemical industry for many years, so inclusion of such activities as a component of meeting RBPS 5 would be a natural application of normal business practices.

Good product stewardship generally allows a facility to know where its product is at all times; ensures that the material is being delivered to or received from a known, approved individual or entity; and helps prevent the theft or diversion of materials through force or deception. Elements that a good Product Stewardship program may contain include:

- Strict vehicle identification and entry authorization, shipping, and control procedures that are subject to a testing program to confirm reliability.
- Procedures for handling the arrival of an unknown carrier at the facility, including the staging of a vehicle and its driver until both the driver and the load are vetted and approved.
- Confirmation by the facility employee responsible for that shipment of feed materials or products to or from the facility that the shipment is expected and approved.
- Advance planning and approval of in-bound and out-bound shipments of hazardous materials such as chemicals of interest.
- An active, documented "know your customer" program that includes a policy of refusing to sell hazardous materials such as chemicals of interest to those who do not meet the pre-established customer qualification criteria. Examples of such criteria may include:
  - verification and/or evaluation of the customer's on-site security
  - verification that shipping addresses are valid business locations
  - confirmation of financial status
  - establishment of normal business-to-business payment terms and methods (e.g., not allowing cash sales)
  - verification of product end-use.
- Proper identification checks and verification of transactions for customer pickup of packaged hazardous materials such as chemicals of interest.
- A review procedure with appropriate redundancies is in place for all shipping, receiving and delivery of hazardous materials such as chemicals of interest.

Inventory Control

There are multiple inventory control systems and relational databases that could be used for tracking hazardous materials such as COI at covered facilities, from single stockrooms to large multi-site enterprise environments. The systems differ in many respects, but generally include the following elements:

- list of all the COI at the covered facility
- provides tracking of the quantity and the physical location of each COI
- monitors use by authorized personnel
- allows generation of reports on COI by location, vendor, name, etc.
- provides container-based tracking of multiple lots, vendors, and sizes
- tracks disposal and maintains a record of disposed containers
- purchasing/receiving records for materials management
- linked to Materials Safety Data Sheets (MSDS) information

More advanced inventory control systems can rapidly detect when hazardous materials such as COI have been removed from their proper locations. Examples of such systems are process controls that monitor the level, weight, volume, or other process parameters which measure the inventory of COI.

Inventory control of hazardous materials such as COI also can be enhanced through the use of physical security and/or control procedures, such as, for example:

- Physical measures and/or procedures that restrict access to storage of COI, allowing access only to authorized individuals
- Performance of background checks on employees with unescorted access to COI;
- Training of employees working in restricted areas to identify and report suspicious behavior.
- Operations or other personnel monitor critical process equipment containing chemical of interest directly via patrols and via CCTV to reduce the potential for tampering or sabotage.
- A locked rack or other tamper-evident, physical means of securing man-portable containers of theft/diversion COI is provided. Examples include
    - chains and locks that cannot be cut or breached with man-powered tools
    - movement alarms on the containers
    - entry/motion detectors and alarms for the buildings or rooms where the containers are stored.
- The drivers transporting theft chemicals of interest are issued facility badges pursuant to 3rd party verification of background suitability or have other proof of suitability, such as a TWIC.
- Vehicle entry and egress is not allowed at an unmanned gate.
- All vehicles are inspected upon egress from the facility or restricted area for theft/diversion chemicals of interest.

Security Considerations

Business Benefits

If done properly, many of the activities that help increase shipping, receipt, and storage security can provide significant benefits on the business side as well, as they often focus on areas such as customer relations, inventory control, and value chain management. When determining what measures and/or processes to implement in regards to this RBPS, a facility's security officer may want to coordinate with the operations and business groups at the facility and/or corporate headquarters to identify what activities can have the most benefit across both fronts.

Layered Security

Completely adequate protection is rarely achievable solely through implementing a single security measure. Rather, an appropriate security solution typically depends upon the use of multiple countermeasures providing "layers of security" for protection. This may include not only the layering of multiple physical protective measures, but also the effective integration of physical protective measures with procedural security measures, including procedures in place before an incident and those employed in response to an incident.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 7: RBPS Metrics – RBPS 5 – Shipping, Receipt, and Storage

RBPS 5 – Shipping, Receipt, and Storage - Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials such as COI that make it extremely unlikely that such materials would be made available to an unauthorized individual or an individual without a legitimate use for the material.	The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials such as COI that make it unlikely that such materials would be made available to an unauthorized individual or an individual without a legitimate use for the material.	The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials such as COI that reduce the likelihood that such materials would be made available to an unauthorized individual or an individual without a legitimate use for the material.	

Table 7: RBPS Metrics – RBPS 5 – Shipping, Receipt, and Storage				
RBPS 5 - Shipping, Receipt, and Storage - Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 5.1 – Security of Transportation Containers On-site	The facility adequately secures all transportation containers of hazardous materials such as COI on-site that are used for storage not incident to transportation, including transportation containers connected to equipment at a facility for loading or unloading and transportation containers detached from the motive power (e.g., a locomotive, truck/tractor) that delivered the container to the facility. Effective security generally includes storing the container within the facility's security perimeter and under the facility's security control, considering the container in the facility's Site Security Plan, and securing and monitoring railcars and other containers using measures consistent with the materials which they contain.			
Metric 5.2 – "Know-Your-Customer" Provisions	The facility has an active, documented "know your customer" program that may include a policy of refusing to sell hazardous materials such as COI to those who do not meet pre-established customer qualification criteria, such as confirmation of identity, verification and/or evaluation of on-site security, verification that shipping addresses are valid business locations, confirmation of financial status, establishment of normal business-to-business payment terms and methods (e.g., not allowing cash sales), and verification of product end-use.			The facility has a "know your customer" program.
Metric 5.3 – Carrier and Shipment Facility Access	The facility has strict vehicle identification and entry authorization, shipping, and control procedures that are subject to a testing program to confirm reliability. If an unknown carrier arrives at the facility, the vehicle and its driver are staged until both the driver and the load are vetted and approved.			The facility has vehicle identification and entry authorization, shipping, and control procedures.
Metric 5.4 – Confirmation of Shipments	The facility has effective security procedures regarding shipments, generally including: • Procedures requiring the relevant facility party to confirm all shipments of feed materials or products to or from the facility before allowing the vehicle or its driver/passengers on-site. • Advance planning and approval of all in-bound and out-bound shipments of hazardous materials such as COI (unannounced shipments are not allowed). • Proper identification checks and verification prior to customer pickup of packaged COI.		The facility has effective security procedures regarding shipments, generally including: • Procedures requiring the relevant facility party to confirm most shipments of feed materials or products to or from the facility before allowing the vehicle or its driver/passengers on-site. • Advance planning and approval of most in-bound and out-bound shipments of hazardous materials such as COI. • Proper identification checks and verification prior to customer pickup of packaged COI.	
Metric 5.5 – Verification of Sales and Orders	A review procedure with appropriate redundancies is in place for all shipping, receiving and delivery of hazardous materials such as chemicals of interest. In particular, the facility has a process to verify receipt of orders for COI and written procedures are in place detailing the specific instructions and requirements to control activities related to sales and storage of COI.			N/A

RBPS 6 – Theft or Diversion

RBPS 6 - Theft and Diversion - Deter theft or diversion of potentially dangerous chemicals

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 6 – Theft or Diversion establishes performance standards focused on preventing the theft or diversion of potentially dangerous chemicals, such as chemicals of interest (e.g., chemical weapons, chemical weapons precursors, explosives, explosive precursors, or other chemicals of interest that could be used to inflict harm at a facility or off-site).

Security Measures and Considerations for Theft or Diversion

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Theft or Diversion performance standards, a facility might consider the following potential attack scenarios:

- Theft/Diversion

Security Measures

The primary means to prevent the theft or diversion of dangerous chemicals such as chemicals of interest is through inventory control systems that can monitor and/or track such chemicals, procedures that make it more

difficult to steal or divert the chemicals and physical measures that make the actual movement of such chemicals more difficult.

Inventory Controls

There are multiple inventory control systems and relational databases used for tracking dangerous chemicals such as chemicals of interest that could be used at covered facilities, from single stockrooms to large multi-site enterprise environments. The systems differ in many respects, but generally have the following elements in common:

- includes lists of all the COI in the covered facility
- provides tracking of the quantity and the physical location of each COI
- monitors use by authorized personnel
- allows generation of reports listing COI by location, vendor, name, etc.
- provides container-based tracking of multiple lots, vendors, and sizes
- tracks disposal and maintains a record of disposed containers
- generates purchasing/receiving records for materials management
- is linked to Material Safety Data Sheets (MSDS) information

Procedural Measures

Procedural measures also can help minimize the ease with which theft or diversion of dangerous chemicals such as COI can occur as well. Measures that a facility might want to consider include:

- Restricting access to areas with COI to authorized personnel only.
- Employing a "two-man rule" whereby no individual is allowed in the area with the COI unescorted.
- Performing background checks on employees with access to COI.
- Training employees working in restricted areas to identify and report suspicious behaviors.
- Prohibiting vehicle entry and egress from unmanned gates.
- Issuing identification badges to drivers transporting COI after the completion of 3rd party verification of background suitability.

Physical Measures

Various physical measures can help minimize the likelihood of theft and diversion of dangerous chemicals such as COI; e.g., limiting access to COI and inhibiting the portability of COI, and monitoring areas containing COI and screening individuals and vehicles. Specific measures a facility may wish to implement include:

- Operations or other personnel monitor locations containing COI directly via patrols and/or via CCTV.
- A locked rack or other tamper-evident, physical means of securing man-portable containers of COI is provided. Examples include:
    - chains and locks that cannot be cut or breached with man-powered tools
    - movement alarms on the containers

- entry/motion detectors and alarms for the buildings or rooms where the containers are stored.

- All vehicles are inspected upon egress from the facility or restricted area for chemicals of interest.

Security Considerations

Business Benefits

If done properly, many of the activities that help increase shipping, receipt, and storage security can provide significant benefits on the business side as well, as they often focus on areas such as customer relations, inventory control, and value chain management. When determining what measures and/or processes to implement in regards to this RBPS, a facility's security officer may want to coordinate with the operations and business groups at the facility and/or corporate headquarters to identify what activities can have the most benefit across both fronts.

Layered Security

Completely adequate protection is rarely achievable solely through implementing a single security measure. Rather, an appropriate security solution typically depends upon the use of multiple countermeasures providing "layers of security" for protection. This may include not only the layering of multiple physical protective measures, but also the effective integration of physical protective measures with procedural security measures, including procedures in place before an incident and those employed in response to an incident.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 8: RBPS Metrics – RBPS 6 – Theft and Diversion

RBPS 6 - Theft and Diversion - Deter theft or diversion of potentially dangerous chemicals				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has multiple, vigorous security measures that are extremely effective in deterring the theft or diversion of dangerous chemicals such as COI.	The facility has multiple security measures that are effective in deterring theft or diversion of dangerous chemicals such as COI.	The facility has security measures that reduce the likelihood of theft or diversion of dangerous chemicals such as COI.	The facility has security measures intended to deter theft or diversion of dangerous chemicals such as COI.

Table 8: RBPS Metrics – RBPS 6 – Theft and Diversion				
RBPS 6 - Theft and Diversion - Deter theft or diversion of potentially dangerous chemicals				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 6.1 – Restricted Access to Dangerous Chemicals	Vigorous controls and procedures exist that restrict access to storage of dangerous chemicals such as COI, allowing access only to authorized individuals.	Controls and procedures exist that restrict access to storage of dangerous chemicals such as COI, allowing access only to authorized individuals.		Controls and procedures exist that restrict access to storage of dangerous chemicals such as COI.
Metric 6.2 – "Know-Your-Customer" Provisions	The facility has an active, documented "know your customer" program that includes a policy of refusing to sell dangerous chemicals such as COI to those who do not meet pre-established customer qualification criteria, such as confirmation of identity, verification and/or evaluation of on-site security, verification that shipping addresses are valid business locations, confirmation of financial status, establishment of normal business-to-business payment terms and methods (e.g., not allowing cash sales), and verification of product end-use.			The facility has a "know your customer" program.
Metric 6.3 – Background Checks	All employees and contractors involved with dangerous chemicals such as COI have undergone background surety investigations and have been trained to identify and report suspicious behaviors. Drivers transporting COI are issued facility badges subsequent to 3rd party verification of background suitability.			
Metric 6.4 – Monitoring Dangerous Chemicals	Personnel monitor critical process equipment containing dangerous chemicals such as COI directly via patrols, CCTV, or other method to reduce the potential for tampering, sabotage or theft. Additionally, security tags (e.g., a Radio Frequency Identification Device (RFID) or similar systems) are attached to or embedded on containers of dangerous chemicals such as COI.		Personnel monitor critical process equipment containing dangerous chemicals such as COI directly via patrols, CCTV, or other method to reduce the potential for tampering, sabotage or theft.	
Metric 6.5 – Physical Security of Dangerous Chemicals	A locked rack or other physical means of securing man-portable containers of dangerous chemicals such as COI is provided. The method(s) used are resistant to breach or tampering. Examples include chains and locks that cannot be cut or breached with man-powered tools, movement alarms on the containers, and entry/motion detectors and alarms for the buildings or rooms where the containers are stored.			
Metric 6.6 – Vehicular Access	Vehicle entry and egress to locations with dangerous chemicals such as COI is through a manned or monitored entry point.			
Metric 6.7 – Vehicle Inspections	All vehicles are inspected upon egress from the facility or restricted area for dangerous chemicals such as COI.	Vehicles are inspected upon egress from the facility or restricted area for dangerous chemicals such as COI on a random basis so that at least 10% of all vehicles are inspected.	Vehicles are inspected upon egress from the facility or restricted area for dangerous chemicals such as COI on a random basis so that at least 5% of all vehicles are inspected.	N/A
Metric 6.8 – Inventory Control	The facility has an inventory control system for dangerous chemicals such as theft COI that can either rapidly detect when such chemicals have been removed from their proper location or are monitored to identify attempts to remove such chemicals in an unauthorized manner. Examples of such systems include process controls that monitor the level, weight, volume, or other process parameters which measure the inventory of theft COIs, or other security measures (e.g., monitoring, access controls) combined with cross-checking of inventory through periodic inventory reconciliation to ensure no product loss.			
Metric 6.9 – Tamper Evident Devices	The facility employs tamper-evident seals for the vehicle valves and other appurtenances that can indicate if a shipment has been tampered with.		N/A	

Table 8: RBPS Metrics – RBPS 6 – Theft and Diversion				
RBPS 6 - Theft and Diversion - Deter theft or diversion of potentially dangerous chemicals				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 6.10 - Cyber Security for Dangerous Chemicals	The facility has implemented appropriate cyber security measures and procedures for business systems that manage the ordering and/or shipping of dangerous chemicals such as theft COI, as well as any other cyber systems that contain personally identifiable information for those individuals who manage critical business systems or who could be exploited to steal or divert dangerous chemicals such as theft COI.			

RBPS 7 – Sabotage

RBPS 7 - Sabotage - Deter insider sabotage

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

Insider sabotage is a deliberate action aimed at weakening an employer through subversion. Deterring insider sabotage prevents the facility's own property and activities from being used by a potential terrorist against the facility. Sabotage is usually associated with the activity of an individual or group whose actions result in the destruction or damaging of a productive or vital facility, and is of particular concern for facilities that are high-risk based on the production of mission critical or economically critical chemicals.

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Sabotage performance standards, a facility might consider the following potential attack scenarios:

- Sabotage

Although most acts of sabotage do not have a primary objective of inflicting casualties, sabotage tied to terrorism may be specifically intended to generate casualties and injuries. Chemicals of interest that have the potential to create significant adverse consequences for human life or health if sabotaged or otherwise contaminated are listed in Appendix A as sabotage chemicals of interest.

Security Measures and Considerations for Sabotage

Security Measures

Examining the background of employees or contractors can greatly reduce the likelihood of insider sabotage, as does ensuring that visitors and contractors have legitimate business on-site and are escorted when necessary. Also restricting access to certain chemicals of interest or to sensitive areas of a facility through administrative controls and physical security measures limits the potential for sabotage. Finally, cyber security measures are the primary means for minimizing a facility's vulnerability to cyber sabotage.

Background Investigations

DHS believes personnel surety to be a key component of a successful chemical facility security program, with the level of screening commensurate with the access provided. Because sabotage is typically done by or with the help of an insider, the performance of background investigations on those individuals with access to sensitive areas of a facility is the best way to prevent sabotage. Background checks can be defined as the process of acquiring information on an individual through third-party services, government organizations, and private individuals to make a "suitability determination" regarding their ability to access sensitive areas. As background investigations are the focus of RBPS 12, significant additional detail on them can be found in the chapter discussing RBPS 12 as well as in Appendix C.

The level and depth of background investigations to reduce the likelihood of sabotage should be tied to the potential severity of the consequences that could occur because of sabotage, and applicable to individuals with potential access to the area or the specific asset capable of generating those undesired consequences.

Visitor Controls

Physical-security precautions against sabotage include the screening, identification, and control of visitors. Visitors are generally classed in the following categories:

- Persons with whom the covered facility has business (such as suppliers, customers, and inspectors)
- Individuals or groups who desire to visit a covered facility for personal or educational, technical, or scientific reasons.
- Individuals or groups specifically sponsored by or representing the government
- Guided tours to selected portions of the covered facility in the interest of public relations

By implementing identification and control mechanisms for visitors, facilities can help mitigate the risks posed by visitors. Identification and control mechanisms to consider include the following:

- Positive identification of visitors
- Contacting facility personnel to validate the visit
- The use of visitor registration forms to provide a record of the visitor and the time, location, and duration of his visit

- The use of visitor cards/badges
- Visitor escort requirements

Physical Security Measures

Physical security measures that make access to areas where sabotage can occur more difficult helps to both deter sabotage attempts and defend against sabotage attempts. Physical security measures that can be used to deter and defend against sabotage come in a variety of types. For more information on standard physical security measures, please refer to RBPS 1, 3 and 4.

Cyber Security Measures

Sabotage can also be performed using cyber means. While background investigations, visitor controls, and physical security measures help protect against physical sabotage, they are of limited value against cyber sabotage attempts. To prevent cyber sabotage, cyber security measures are needed. An in depth discussion of various cyber security measures and policies that a facility may want to employ is contained in RBPS 8 – Cyber, as well as in Appendix C.

Security Considerations

Layered Security

Completely adequate protection is rarely achievable solely through implementing a single security measure. Rather, an appropriate security solution typically depends upon the use of multiple countermeasures providing "layers of security" for protection. This may include not only the layering of multiple physical protective measures, but also the effective integration of physical protective measures with procedural security measures, including procedures in place before an incident and those employed in response to an incident.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 9: RBPS Metrics – RBPS 7 – Sabotage				
RBPS 7 - Sabotage - Deter insider sabotage				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has procedures and security measures in place that are effective at deterring, detecting, delaying and responding to sabotage.			The facility has procedures and security measures in place that are aimed at deterring, detecting, delaying and responding to sabotage.

Table 9: RBPS Metrics – RBPS 7 – Sabotage				
RBPS 7 - Sabotage - Deter insider sabotage				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 7.1 – Procedures	The facility has procedures in place to deter, detect, delay, and respond to sabotage, such as routine equipment inspections for tampering, awareness training, process safety measures, restricted access to sensitive areas, and protocols for verifying the identity and shipment orders of carriers who arrive to remove transportation containers of sabotage COI from the facility.			
Metric 7.2 – Tamper Evident Devices	The facility utilizes active tamper-evident devices to secure designated target asset (e.g., sabotage COI) transportation containers. The devices(s) used are fairly resistant to breach or tampering and indicate when attempts to tamper with the containers has occurred. Examples include car seals or other tamper-indicating devices, physical locks on transportation container valves or access hatches/openings, chains and locks that cannot readily be cut or breached with man-powered tools, alarms on the valves or access hatches/openings of the transportation containers, entry/motion detectors and alarms for the buildings or rooms where the transportation containers are stored.			
Metric 7.3 – Visitor Controls	The facility has documented and implemented strict visitor identification, escort, and access control procedures that include verification of visitor background suitability or constant visitor escort by appropriately vetted personnel in restricted areas.	The facility has documented and implemented visitor identification, escort, and access control procedures that include verification of visitor background suitability or constant visitor escort by appropriately vetted personnel in restricted areas.	The facility has documented and implemented visitor identification, escort, and access control procedures.	The facility has implemented visitor identification, escort, and access control procedures.

RBPS 8 – Cyber

RBPS 8 - Cyber – Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems.

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

Cyber systems (e.g., Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems) are integrated throughout the operations of chemical facilities, including controlling sensitive processes, granting authorized access, and enabling business. Protecting against cyber sabotage of these systems is an essential component in managing overall risk for a facility. A comprehensive approach of appropriate security policies, practices, and people to prevent, protect, respond, and recover from incidents deters cyber sabotage.

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Cyber performance standards, a facility might consider the following potential attack scenarios:

- Sabotage
- Theft/Diversion

Cyber systems that a facility may wish to consider critical for purposes of this RBPS include but are not limited to those that:

- monitor and/or control physical processes that contain a chemical of interest;

- are connected to other systems that manage physical processes that contain a chemical of interest; or
- contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a chemical of interest.

A facility's critical cyber systems can be located and managed at its campus or outside the geographic boundaries of its location (e.g., at corporate headquarters or a vendor's location). The following lists provide examples of critical and non-critical cyber systems. These lists are not inclusive of all potentially critical or non-critical cyber systems and are provided only to help facilities better understand and identify critical cyber systems covered under the CFATS.

Examples of cyber systems that a facility may wish to consider critical (e.g., in the context of a chemical of interest) could include:

- A control system that directly monitors and/or controls manufacturing or other physical processes that contain COI
- A business system at the headquarters that manages ordering and/or shipping of a COI
- A business system (at the facility, headquarters, or outsourced) that contains personally identifiable information of those individuals who could be exploited to steal, divert, or sabotage a COI
- An access control or security monitoring system that is connected to other systems
- Enterprise resource planning systems that conduct critical functions in support of chemical processes for COI or a COI supply chain activity
- E-mail and fax systems used to transmit sensitive information related to ordering and/or shipping of a COI
- A remotely-operated control system that monitors and or controls a process containing a COI
- A non-critical control system on the same network as a critical control system
- A sales system that is connected to the data historian for a critical control system
- A watch-dog system for a critical control system
- A system hosting critical or sensitive information that, if exploited, could result in the theft or diversion of a COI or sabotage its processing (e.g., website, intranet)

Examples of cyber systems that a facility likely would not consider critical in the context of a COI could include:

- A control system that is not connected to any critical systems
- A business system at the headquarters that contains no personally identifiable information
- An access control or security monitoring system that is not connected to other systems or networks
- A sales system that is not connected to the data historian for a critical control system
- A financial system for the facility/organization
- A system hosting non-critical and non-sensitive information about the facility (e.g., website, intranet)

Security Measures and Considerations for Cyber

Security Measures

Effectively securing a facility's cyber systems from attack or manipulation typically includes a combination of policies and practices in several categories: (1) security policy, (2) access control, (3) personnel security, (4) awareness and training, (5) monitoring and incident response, (6) disaster recovery and business continuity, (7) system development and acquisition, (8) configuration management, and (9) audits. The following subsections provide brief descriptions of each of those cyber security areas. Additional detail on each can be found in Appendix C.

Security Policy

Security policies, plans, and procedures. Security policies, plans/processes, and procedures that specifically address operational constraints, sensitivity issues, and processing environment issues are common starting points for cyber security, whether they are addressed in general information technology (IT) documentation or contained in their own dedicated documentation. One security policy document that is especially worthwhile is a formal change management process. Without a defined process that takes into account policy mandates, security concerns, business impact, authorization, and oversight, changes can weaken the stability and security of a system. Development and distribution of a cyber change management process supports the achievement of the most effective and efficient application of network and system updates, reduces the likelihood of the introduction of malicious code, and reduces the chance of human error. In addition to procedural documents governing the change management process, audit logs documenting who made changes to what and when also are useful tools.

Cyber Security Officials. Designating an individual to be responsible for cyber security often helps establish management support for cyber security as well as providing direction, accountability, and oversight to cyber security. Examples include a Chief Information Officer, an IT Cyber Security Specialist, or a System Administrator.

Access Control

System Boundaries. The process of uniquely assigning information resources/assets to a cyber system defines the boundaries for that system. While some systems may be defined by lines of direct management control, it is also possible for system boundaries to be established based on functional or business purpose. Facilities have flexibility in determining what constitutes the boundaries of a cyber system and should consider factors that promote effective information security.

External Connections. Understanding and managing connectivity—i.e., the possibility of transferring data electronically (e.g., through external access such as the wireless connection or portable cyber equipment such as flash drives)—is typically an essential component of cyber security. Because cyber vulnerabilities can be exploited in many ways, connectivity is not as simple as whether or not a wired connection to the Internet is openly in use. Network back doors exist in the form of wireless connections, modems, portable electronic devices and media such as laptop computers, personal digital assistants (PDA), universal serial bus (USB) drives, compact disks (CD), or floppy disks, etc. By verifying external connections through the use of network tools designed

for this purpose, managers can greatly increase the security environment of their systems and networks.

Business and control networks often are connected for efficiency or economy, or because common or public networks are used for communications or as integral parts of the larger system. Unfortunately, this opens the control systems network to the vulnerabilities of the general business infrastructure, including the Internet—issues for which they typically were not designed, and often are not managed. Firewalls can be used to control access, but most firewalls common in the industry today do not inspect for valid control system protocol contents, thus frequently making the firewall an ineffective barrier between the systems. Other methods exist for configuring the networks to limit access to control systems, e.g., segregating business and control networks, but this may impact efficiency or economy. For these reasons, a good cyber security posture typically will include rules governing system interconnection, especially when connections exist to components outside of an organization's direct control.

Remote Access and Rules of Behavior. Remote access (e.g., via the Internet, Virtual Private Network, modems) occurs when users (e.g., employees, vendors, maintenance personnel, and others) access or communicate with a cyber system outside of a facility where that cyber system resides. Rules of behavior are often established by the facility and made available to all cyber system users. Those rules typically describe user responsibilities, expected behavior with regard to information system usage (e.g., appropriate web sites, conduct of personal business), including remote access activities.

Least Privilege. Facilities are encouraged to employ the "least privilege" concept (i.e., granting people only as much access as they need to perform their assigned job function and no more).

Password Management. Managing passwords is a key component of a good cyber security program. Password management often includes immediately changing all default passwords provided with any systems or applications, and establishing parameters and rules for password structure. Typically, parameters take into account not only the structure of the password (e.g., requiring at least one uppercase and one lower case letter), but also the frequency of password changes (e.g., requiring a user to change his or her password every 90 days). In instances where changing default passwords is not technically feasible (e.g., a control system with a hard-coded password), then appropriate compensating security controls (e.g., physical controls) are often implemented.

Personnel Security

Criticality Sensitivity Review. It is a good cyber security practice to review all roles to determine what types/levels of sensitive materials someone filling that role is allowed access to. Assigning a "high," "medium," or "low" rating to a role is a common labeling process, and can be very useful so long as those terms are well defined for the business. An example rating would be a rating of high for system administrators.

Unique Accounts. Organizations typically establish unique accounts for each individual user in order to provide appropriate access and accountability. When accounts are shared among multiple individuals, it cannot be determined which user is responsible for a given action. Additionally, if a security breech occurs it can be difficult to identify the source of that breech if it comes from a

shared account. Accordingly, it is generally good cyber security practice to use individual user accounts where technically feasible.

In some control systems environments, it may be standard practice to use a single group account for multiple users. Management may make a risk based decision to allow this practice for business purposes; however, the risk associated with that decision should be managed with appropriate compensating controls.

Separation of Duties. Although people often play multiple roles within an organization, it is generally a good idea to have each of these roles, and their related security needs, defined and separated as much as possible. This allows for natural checks-and-balances, which is important for preventing human error and internal misuse of systems and information. A balance between what is good for security and what access is needed to allow business to be conducted smoothly is often the goal.

Access Control Lists. Actively managing access for changing roles of employees (e.g., termination, transfer) is one way to ensure that only appropriate access is allowed. Immediate review of all role changes is recommended. For all employees who have departed under adverse circumstances, however, it is recommended that all access rights (both physical and electronic) be revoked by close of business the same day.

Third-party Cyber Support. Managing relationships with external service providers, business partners, and vendors should be considered so that they do not compromise the security of an organization.

Physical Access to Cyber Systems and Information Storage Media. Marking and otherwise restricting specific physical areas where cyber systems and information storage media are located or managed in a facility can greatly improve security. Combined with a role based security model, personnel can know where they are and are not allowed.

Awareness and Training

The human component is often the most vulnerable aspect of a system. As a result, a good cyber security program generally involves making system users aware of the need for security and instructing them on their roles in keeping the cyber system secure. A documented cyber security training program, which establishes the types and frequency of training, is one effective way to accomplish this. Basic topics that a facility may want all employees to receive could include:

- General company policy review
- Roles and responsibilities
- Password procedures
- Acceptable practices
- Whom to contact and how to report suspected inappropriate or suspicious activity.

Training is most effective when refreshed and reinforced on a predetermined schedule, and when updated to reflect the changing threat and vulnerability environment. An effective training program may provide for different training regimens for employees based on their differing roles.

Cyber Security Controls, Monitoring, Response, and Reporting

Cyber Security Controls. Viruses, worms, Trojan Horses, and other malicious software code proliferate on the Internet and mutate on an unpredictable basis. Malicious code is so common that without automated protection it is a near certainty that systems will be infected. Even without access to the Internet, malicious code can be introduced to an organization through actions (even unintended) of employees, support personnel, vendors, and business partners. Antivirus software can be implemented on a facility's systems when architecture and application permit it, and such software should be updated on a regular basis, preferably automatically. Additionally, with the prevalence of e-mail borne viruses and other spam messages including malicious software attachments, owner/operators should consider filtering e-mail attachments.

For control systems where system architectures or operational requirements may not permit the use of antivirus software, layered defenses can be used to prevent events or intrusions from reaching vulnerable control systems.

Network Monitoring. Facility's monitor networks for unauthorized or malicious access to maintain situational awareness and mitigate risk. An intrusion detection system (IDS) can be used to monitor networks. IDS are designed to capture network or host traffic, analyze it for known attack patterns, and take specified action when it recognizes an intrusion or attempted intrusion. An IDS can be software or hardware, and can be network-based or host-based. Recognizing and logging events and incidents is a critical component of network monitoring.

Incident Response. Incident response is an important part of a comprehensive cyber security program, and a good cyber security program typically will include a defined Computer Emergency Response function that can be contacted in the event of a cyber emergency and that is specially trained to identify, contain, and resolve a cyber intrusion, denial of service attack, virus, worm attack, or other cyber incident.

Incident Reporting. Recognizing security events and making management and the DHS United States Computer Emergency Readiness Team (US-CERT) (www.us-cert.gov) aware of the incidents and their potential for harm is an important element in obtaining the appropriate support and resources to effectively manage cyber security, thus limiting the damage from future cyber attacks.

Safety Instrumented Systems. Safety Instrumented Systems (SIS) are systems that take action when something goes wrong on a cyber system and process conditions go outside the normal operating envelope. An SIS typically provides interlocks or responses to prevent or mitigate catastrophic events and/or consequences of a cyber attack. An SIS is an independent system implemented for the purpose of taking a process to a safe state when pre-determined conditions are violated. When networked with the control systems they stand to protect, an SIS may be subject to the exploitation of the same vulnerabilities if not appropriately secured.

Disaster Recovery and Business Continuity

Post-Incident Measures. A good cyber security posture typically includes: Continuity of Operations Plans (COOP), IT Contingency, and Disaster Recovery Plans for its critical cyber assets, all of which incorporate cyber security considerations during contingency operations and recovery/reconstitution activities. As recovery operations (i.e., those operations addressed in COOP, IT Contingency, and Disaster Recovery Plans) are often done under pressure, systems often

are vulnerable to security concerns when they are underway, and thus it is important to consider cyber security during such operations.

System Development and Acquisition

Systems Lifecycle. Including cyber security throughout the system development lifecycle, from system design through procurement, implementation, operation, and disposal, is generally part of good cyber security. By integrating system security into the existing development lifecycle, a facility can ensure that money is budgeted, personnel are designated, and requirements are gathered for security at appropriate times.

Configuration Management

Cyber Asset Identification. Maintaining a current inventory of hardware (e.g., cyber systems, networks, network devices, media devices), software (e.g., applications), information (e.g., critical information), and services (e.g., virus checking) on the network has numerous benefits. Network elements can be located, tracked, diagnosed, and maintained with far greater efficiency than if not documented. The vulnerabilities of network elements are identified and evaluated for applicability to the operating environment, and then factored into a risk-management decision.

Network/System Architecture. A cohesive set of network/system architecture diagrams or other documentation including nodes, interfaces, and information flows ensures a comprehensive understanding of connectivity, dependency, and security vulnerability based on the system's current operating environment.

Audits

Audits are generally important to maximize the effectiveness of the cyber security measures that have been put in place. Facilities with strong cyber programs typically will report the results of audits to senior management so that findings can be understood and agreed upon, and mitigated with management support.

Security Considerations

Potential Off-site Aspect of Cyber Security

Given the nature of today's information technology environment, it is not unusual for IT equipment, IT data, or even IT staff to be located off-site. For instance, corporations with multiple facilities may keep central data servers and processing units in a single location at one facility, may only have cyber security officers and other cyber staff located at corporate headquarters, and may have backup data stored at facilities managed by third parties. End users connected to a facility's cyber system may be scattered not only across the country, but even outside of the United States. As a result, facility cyber security often is not limited to the physical site of the facility itself. Good cyber security practices include a facility taking a comprehensive view of all its cyber assets, whether equipment, people, or data, and whether located on-site, at corporate headquarters, or elsewhere.

Interconnectivity of Critical and Seemingly Non-Critical Systems

Often, a facility's numerous cyber systems may be interconnected in one form or another. If connected, some seemingly non-critical systems may warrant additional security attention as they are a potential avenue for access to systems that manage critical processes, such as a process involving a chemical of interest. When analyzing the security posture of a critical system, it is important to identify connected systems and review their security as well.

Impact of Risk Drivers

As in the world of physical security, facility characteristics have a great deal of impact on the appropriate cyber security posture for a facility. For example, if the facility is high-risk due to a release hazard, it likely needs to focus cyber security on its process control systems, as well as those cyber systems that assist in controlling access to the facility. However, if theft/diversion is the risk driver, then securing cyber business systems to ensure that shipments and customers are proper may be more important than securing the process control systems.

Physical Security for Cyber Assets

Cyber systems can not only be compromised electronically, but also can be compromised physically. Accordingly, physically protecting critical cyber assets is a key component of a comprehensive cyber security program. Marking and otherwise restricting specific physical areas in a facility can greatly improve security when combined with a role-based security model where all personnel know exactly where they are and are not allowed. Accordingly, when implementing physical security measures pursuant to other RBPSs, it is a good idea to consider physical security for sensitive cyber assets such as control rooms, LAN and server rooms, and wiring closets.

Layered Security

Completely adequate protection is rarely achievable solely through implementing a single security measure. Rather, an effective security solution typically depends upon the use of multiple countermeasures providing "layers of security" for protection. This may include not only the layering of multiple physical protective measures, but also the effective integration of physical protective measures with cyber and procedural security measures, including procedures in place before an incident and those employed in response to an incident.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 10: RBPS Metrics – RBPS 8 – Cyber				
RBPS 8 - Cyber – **Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems.**				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility should have in place cyber security policies, procedures, and measures that result in a low risk of a successful attack on the facility's critical cyber systems or using a facility's critical cyber systems to carry out or facilitate an attack.			
8.1 Cyber Security Policies				
Metric 8.1.1 – Security policies, plans, and procedures	The facility should have documented and distributed cyber security policies (including a change management policy), plans/processes and supporting procedures commensurate with the facility's current IT operating environment.		The facility should have documented and distributed cyber security policies (including a change management policy) or plans/processes commensurate with the facility's current IT operating environment.	
Metric 8.1.2 – Cyber Security Officials	The facility should designate an individual(s) to manage cyber security for the facility who can demonstrate proficiency through a combination of training, education, and/or experience sufficient to develop cyber security policies and procedures, and ensure compliance with all applicable industry and governmental cyber security requirements.			
8.2 Access Control				
Metric 8.2.1 – Systems Boundaries	The facility should identify and document systems boundaries (i.e., the electronic perimeter) and implements security controls to limit access across those boundaries.			
Metric 8.2.2 – External Connections	The facility should establish and document a business requirement for every external connection to/from their critical systems, and external connections should have controls which permit access only to authorized and authenticated users.			
Metric 8.2.3 – Least Privilege	The facility should practice the concept of least privilege.			
Metric 8.2.4 – Remote Access and Rules of Behavior	The facility should define allowable remote access (e.g., Internet, Virtual Private Network, modems) and rules of behavior. Those rules describe user responsibilities, expected behavior with regard to information system usage, to include remote access activities (e.g., appropriate web sites, conduct of personal business).			
Metric 8.2.5 – Password Management	The facility should document and enforce authentication methods (including password structures) for all administrative and user accounts. Additionally, the facility should change all default passwords and ensure that default passwords for new software, hardware, etc. are changed upon installation. In instances where changing default passwords is not technically feasible (e.g., a control system with a hard-coded password), then the facility may wish to implement appropriate compensating security controls (e.g., physical controls).			
8.3 Personnel Security				
Metric 8.3.1 – Criticality Sensitivity Review	The facility should review and establish security requirements for positions that permit administrative access to critical cyber systems.			
Metric 8.3.1 – Unique Accounts	The facility should establish and enforce unique accounts for each individual user and administrator, should establish security requirements for certain types of accounts (e.g., administrative access to the system), and should prohibit the sharing of accounts. In instances where users function as a group (e.g., control system operators) and user identification and authentication may be role based, then appropriate compensating security controls (e.g., physical controls) should be implemented.			
Metric 8.3.2 Separation of Duties	IT management, systems administration, and IT security duties should be divided amongst three different individuals. In instances where this is not feasible, then appropriate compensating security controls (e.g., administrative controls) should be implemented.		IT management, systems administration, and IT security duties should not be performed by the same individual. In instances where this is not feasible, then appropriate compensating security controls (e.g., administrative controls such as review and oversight) should be implemented.	

Table 10: RBPS Metrics – RBPS 8 – Cyber				
RBPS 8 - Cyber – **Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems.**				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 8.3.3 – Access Control Lists	The facility should maintain access control lists, and ensures that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated in a timely manner (e.g., by close of the business the same day for personnel leaving under adverse action and within one business day when users no longer require access (e.g., when personnel leave the company, complete a transfer into a new role, or their responsibilities change).		The facility should maintain access control lists, and ensures that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated in a timely manner (e.g., by close of the business the same day for personnel leaving under adverse action and within one week when users no longer require access (e.g., when personnel leave the company, complete a transfer into a new role, or their responsibilities change).	
Metric 8.3.4 – Third-party Cyber Support	The facility should ensure that service providers and other third parties with responsibilities for cyber systems have appropriate personnel security procedures/practices in place commensurate with the personnel surety requirements for facility employees.			
Metric 8.3.5 – Physical Access to Cyber Systems and Information Storage Media	The facility should have role-based physical access controls to restrict access to critical cyber systems and information storage media.			
8.4 Awareness and Training				
Metric 8.4.1 – Cyber Security Training	The facility should ensure that employees receive role-based cyber security training applicable to their responsibilities on an annual basis and before obtaining access to the facility's critical cyber systems.		The facility should ensure that employees receive role-based cyber security training applicable to their responsibilities on an annual basis and within 30 days of obtaining access to the facility's critical cyber systems.	
8.5 Cyber Security Controls, Monitoring, Response, and Reporting				
Metric 8.5.1 – Cyber Security Controls	The facility should implement cyber security controls to prevent malicious code from exploiting critical cyber systems, and apply appropriate software security patches and updates to systems as soon as possible given critical operational and testing requirements.			
Metric 8.5.2 – Network Monitoring	The facility should monitor networks near real time for unauthorized access or introduction of malicious code with immediate alerts and should log cyber security events, review the logs daily, and respond to alerts in a timely manner. Network monitoring may occur on-site or off-site. Where logging of cyber security events on their networks is not technically feasible (e.g., logging degrades system performance beyond acceptable operational limits), then appropriate compensating security controls (e.g., monitoring at the network boundary) should be implemented.		The facility should monitor networks for unauthorized access or introduction of malicious code and should log cyber security events, review the logs weekly, and respond to alerts in a timely manner. Network monitoring may occur on-site or off-site. Where logging of cyber security events on their networks is not technically feasible (e.g., logging degrades system performance beyond acceptable operational limits), then appropriate compensating security controls (e.g., monitoring at the network boundary) should be implemented.	
Metric 8.5.3 – Incident Response	The facility should have a defined 24x7x365 computer incident response capability for cyber incidents.		The facility should define computer incident response capability for cyber incidents.	

Table 10: RBPS Metrics – RBPS 8 – Cyber				
RBPS 8 - Cyber – **Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems.**				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 8.5.4 – Incident Reporting	Facility should ensure significant cyber incidents are reported to senior management and the DHS United States Computer Emergency Readiness Team (US-CERT) at www.us-cert.gov.			
Metric 8.5.5 – Safety Instrumented Systems	Facilities with control systems that have safety instrumented systems (SIS) should configure the SIS so that they have no unsecured remote access and cannot be compromised through direct connections to the systems managing the processes they monitor. *Note: this metric only applies to control systems*			
8.6 Disaster Recovery and Business Continuity				
Metric 8.6 – Post-Incident Measures	The facility's alternate facility operations and primary facility recovery/reconstitution phases should include cyber security measures consistent with those in place for the original operational functions.			
8.7 System Development and Acquisition				
Metric 8.7 – Systems Lifecycle	The facility should integrate cyber security into the system lifecycle (design, procurement, installation, operation, disposal). The facility should establish security requirements for all systems and networks before they are put into operation, and for all operational systems and networks throughout their lifecycle.			
8.8 Configuration Management				
Metric 8.8.1 – Documenting Business Needs	The facility should document a business need for all networks, systems, applications, services, and external connections.			
Metric 8.8.2 – Cyber Asset Identification	The facility should identify hardware, software, information, and services and disable all unnecessary elements where technically feasible. The facility should also identify and evaluate potential vulnerabilities and implement appropriate compensating security controls.			
Metric 8.8.3 – Network/ System Architecture	The facility should have an asset inventory of all critical IT systems and a cohesive set of network/system architecture diagrams or other documentation including nodes, interfaces, and information flows.		The facility should have an asset inventory of all critical IT systems.	
8.9 Audits				
Metric 8.9 – Audits	The facility should conduct annual audits that measure compliance with the facility's cyber security policies, plans, and procedures and reports audit results to senior management.		The facility should conduct triennial audits that measure compliance with the facility's cyber security policies, plans, and procedures and reports audit results to senior management.	

RBPS 9 – Response

RBPS 9 – Response – Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 9 – Response sets the performance standard for the development and exercising of emergency response plans for security incidents at the facility. Emergency response within this context primarily refers to the response of appropriately trained personnel (either facility personnel or external first responders) to a fire, aerial release or other loss of containment of a chemical of interest, or similar results of a security incident. This includes plans to mitigate and/or respond to the consequences of a security incident, and to report security incidents internally and externally in a timely manner. The security response to the incident itself and the adversaries perpetrating it is covered in RBPS 4.

Security Measures and Considerations for Response

In the context of this RBPS, "response" includes actions to mitigate the consequences of adversary actions, including those actions assigned to local law enforcement or other off-site emergency responders. Because the RBPS applies to a wide variety of facilities with chemicals of interest, security measures are likely to address the identification of the hazards, planning for effective response, identification of the number and capabilities of the various responders to different types

of adversary events, and the equipping and training of response personnel to maximize their efficiency.

Security Measures

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Response performance standards, a facility might consider the following potential attack scenarios:

- Aircraft
- Assault Team
- Maritime
- Sabotage
- Stand-Off
- Theft/Diversion
- VBIED

Sound physical security measures and personnel who understand the threat and the need for timely, effective actions, when coupled with well-rehearsed response plans, reduce the probability of attack success and mitigate the consequences of a terrorist event. Practiced response plans help ensure that the emergency-response units from local law enforcement, fire fighting, ambulance, mutual aid, rescue, and explosive ordnance device mitigation (bomb-squads) are not impeded from reaching the location of the security event. Drills and exercises test response plan capabilities and identify suspected vulnerabilities. Drills and exercises (see RBPS 11 – Training) also train staff and reaction-group leadership to identify and adjust to changes in threats and adversary capabilities.

Emergency Plans and Processes

One of the most important elements for a successful response to an incident is a well-thought out, documented crisis management plan for responding to an incident, upon which the relevant individuals have been trained. Types of activities a facility may want to address in its overarching crisis management plan to help it in the event of a security breach or other incident include:

- contingency plans
- continuity of operations
- emergency response
- post-incident security (e.g., post-terrorist attack, security incident, accident, hurricane, or other natural disaster)
- evacuation
- notification control and contact requirements
- re-entry
- security response

Crisis management plans generally include any documented agreements with off-site responder services, such as ambulance support, environmental restoration support, explosive device disposal support, fire fighting support, hazardous material spill/recovery support, marine support, and medical support. Crisis management plans also typically include specific roles and responsibilities for the crisis management team, the incident commander, the on-scene commander, operational control and timekeeping.

Training, drills, and exercises

The best plans are of limited value in a crisis if the individuals who are to implement them are not prepared to do so. Consequently, proper training, drills, and exercises are a critical part of any adequate response capability. Training, drills, and exercises are the subject of their own RBPS, and additional details on each can be found in Chapter 11 – Training, as well as in Appendix C.

Emergency Response Equipment

The following equipment can be valuable in helping a facility successfully respond to a security incident:

- A radio system that is redundant and interoperable with law enforcement and emergency response agencies.
- Back up communications systems such as cell phones and desk phones.
- An emergency notification system (e.g., a siren or other facility-wide alarm system)
- Automated control systems or other process safeguards for all process units to rapidly place the designated target asset equipment in a safe and stable condition, and procedures for their use in an emergency.
- Emergency safe shutdown procedures for all process units.
- Emergency back up power for all communications, emergency notification, security systems, and process control systems and/or an equivalent written contingency procedure in place that is designed, laid-out, and constructed to avoid common cause/dependent failures and equipped with redundant signal processing.

Security Considerations

Emergency Response vs. Security Response

It is important not to confuse "security response" intended to engage and hopefully neutralize the adversaries, from the broader "emergency response" following an attack that attempts to reduce the severity of the event and lessen the consequence in terms of loss of life and destruction of property or production capability. The initial "security response" has tactical considerations addressed in RBPS 4 – Deter, Detect, and Delay - whereas the "emergency response" relates to the more traditional efforts to contain the damage and lessen the consequences after a security event. These planning considerations overlap to some degree, and both involve establishing strong, functional, relationships with the various response organizations and personnel that may be needed to support this performance standard.

Backup Power, Communications, and Process Safeguards

In the event of a security incident, some of the basic services typically required to respond to an event—e.g., power, communications—may be disrupted. When designing a crisis management plan, a facility may want to consider whether it has back-up power for security and back-up communications systems (as well as the power to run them).

Similarly, having a procedure for safe shutdown that takes several hours or days, while effective for some accidents or other safety incidents, may not suffice in the case of a security incident. Thus, a facility may want to review its process safeguards—e.g., "process controls" that safely and quickly shutdown a process involving chemicals of interest—and examine whether they can be implemented quickly with less than ideal power, communications, or other support systems.

A facility may want to take these extenuating circumstances into account when designing and performing emergency response training and drills. It generally is most effective for training and drills to realistically exercise the capabilities and flexibility of the response organizations to address multiple, higher-order security events.

Collaboration with Local Law Enforcement and other First Responders

Including local law enforcement and first responders (e.g., emergency medical technicians (EMTs), fire, hazmat) in the development and exercising of an emergency plan can have significant benefits for the facility. In addition to helping the facility prepare to take quick and decisive action in the event of an attack or other breach of security, establishing relationships with local law enforcement improves responder understanding of the layout and of hazards associated with the facility. The first time the local law enforcement, fire, or EMT entities responsible for responding to incidents at a facility access the facility should not be the day of a security incident.

Interrelation to Safety Planning

Most of the measures, activities, and procedures that are useful in responding to security incidents are equally useful when the incident is caused by an accident, natural disaster, or other reason. Accordingly, when developing response plans, training individuals on proper response techniques, or procuring equipment to use during responses, security personnel should consider coordinating with the facility's process safety engineer or other individual in charge of safety at the facility.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 11: RBPS Metrics – RBPS 9 – Response				
RBPS 9 – Response – Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has a documented, comprehensive crisis management plan that details how the facility will respond to security incidents, and regularly runs exercises and drills to improve its ability to implement the plan.			The facility has a documented crisis management plan that details how the facility will respond to security incidents, and runs exercises and drills to improve its ability to implement the plan.
Metric 9.1 – Comprehensive Crisis Management Plan	The facility has a comprehensive crisis management plan that may include: • Documented agreements and/or written procedures for emergency response, including off-site responder services such as ambulance support, explosive device disposal support, fire fighting support, and hazardous material spill/recovery support, and medical support. • Roles and responsibilities for the crisis management team, the incident commander, the on-scene commander, operational control and timekeeping. • Contingency plans, continuity of operations plan, emergency response plans, evacuation plans, media response plans, notification control and contact requirements, re-entry plans, and security response plans. • Emergency safe shutdown procedures for critical process units, such as those processing chemicals of interest.			The facility has a comprehensive crisis management plan that may include: • Documented agreements and/or written procedures for emergency response, including off-site responder services, such as ambulance support, explosive device disposal support, fire fighting support, and hazardous material spill/recovery support. • Documented emergency response plans.
Metric 9.2 – Communication Systems	The facility has a communications and emergency notification system with emergency back up power and/or an equivalent written contingency procedure in place that is designed, laid-out, and constructed to avoid common cause/dependent failures and equipped with redundant signal processing. A typical system includes: • An emergency notification system (e.g., siren or other facility-wide alarm system). • A redundant radio system that is interoperable with law enforcement and emergency response agencies. • Other back up communications systems such as cell phones or desk phones.			The facility has a redundant communications system and an emergency notification system (e.g., siren or other facility-wide alarm system).
Metric 9.3 – Process Safeguards	All process units have an automated control system or other process safeguards to rapidly place designated target asset (e.g., COI) equipment in a safe and stable condition, and procedures for their use in an emergency. Additionally, all process units have a procedure for safe shutdown in an emergency.			
Metric 9.4 – Outreach	The facility has an active outreach program to the community and local law enforcement and emergency responders. Examples of outreach activities include participation in Local Emergency Planning Committee (LEPC) (where local law enforcement is a LEPC member), Community Hazards Emergency Response-Capability Assurance Process (CHER-CAP) (where local law enforcement is a CHER-CAP member), Buffer Zone Protection Program (BZPP) activities, Neighborhood Watch Programs (where industry and businesses are included in these programs), or participation by the facility in security-related drills and exercises in conjunction with off-site responder organizations.			

RBPS 10 – Monitoring

RBPS 10 – Monitoring - Maintain effective monitoring, communications and warning systems, including:
(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;
(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and
(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

Maintaining effective monitoring, communications and warning systems allows the facility to notify internal personnel and local responders in a timely manner about security incidents. Regular tests, repairs and improvements to the warning and communications system increase the reliability of such systems and will improve response time. Complying with the manufacturers' instructions and specifications for frequency of testing, repair and replacement schedules increases the likelihood that the physical security equipment will function as it is expected to and decreases the likelihood that it will malfunction. Instituting a regular, written plan for the maintenance, testing, calibration and inspection of equipment will help ensure that such activities take place as equipment that is functioning well is often overlooked. Records of maintenance, testing and calibration of security equipment must be maintained as specified in 6 CFR §27.255(a)(4).

Security Measures and Considerations for Monitoring

Security Measures

Maintaining effective monitoring, communications and warning systems includes taking steps designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained; regularly testing security systems; noting deficiencies; correcting detected deficiencies; recording results so that they are available for inspection by the Department; and prompt identification and response to security system and equipment failures or malfunctions. To meet these objectives, it is recommended that a facility:

- Develop a written procedure to regularly inspect, test, calibrate, repair and maintain security systems and systems related to security, such as communications and emergency notification equipment. The procedure should identify responsibilities, tasks, their frequencies, and the documentation required.
- Perform inspection, testing, and maintenance tasks on a regular basis and in accordance with the manufacturer's instructions.
- Include all security equipment such as gates, cameras, lights, alarms, and keypad entry systems, in the routine inspection and maintenance.
- Employ appropriate temporary security measures when performing maintenance, as well as in response to non-routine outages, equipment failures and malfunctions.
- Document non-routine incidents and promptly report them to the Site Security Officer (SSO).
- Have procedures to verify the identity and each occurrence of contractor personnel who perform inspection, testing, and maintenance of security equipment (other than resident contractors who are included in the personnel surety program in RBPS 12).

Security Considerations

Manufacturer's Recommendations

Typically, most security equipment comes with manufacturer's recommendations as to the types of testing, inspection, calibration, and maintenance that should be performed and the frequency with which those activities should be performed. Generally speaking, it is a good idea to perform these activities in accordance with the manufacturer's instructions and as frequently as the manufacturer recommends. If a piece of security equipment comes without such instructions, a facility may want to contact either the manufacturer or the vendor from whom they got the equipment to ascertain whether or not there are any specific activities that they recommend be performed.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS.

However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 12: RBPS Metrics – RBPS 10 – Monitoring				
RBPS 10 – Monitoring - Maintain effective monitoring, communications and warning systems, including: (i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained; (ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and (iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has a written plan to regularly inspect, test, calibrate and maintain security systems.			
Metric 10.1 – Inspection, Testing, and Preventative Maintenance (ITPM) Procedures	The facility has written procedures, including responsibilities, tasks, and frequencies, to regularly inspect, test, calibrate, repair and maintain security systems (e.g., gates, cameras, lights, alarms, keypad entry systems) and related equipment such as communications and emergency notification equipment. Typically, a facility bases its ITPM process on the tasks and their frequencies identified in the manufacturer's recommendations; where the manufacturer has not made ITPM recommendations, the tasks and their frequencies often are based on the operating history of the equipment, its operating environment, the redundancy installed, and other factors as approved by the Site Security Officer.			
Metric 10.2 – Outages	Appropriate temporary security measures are implemented in response to non-routine outages, equipment failures and malfunctions, and such incidents are documented and promptly reported to the Site Security Officer.			
Metric 10.3 – Repairs	The facility has a written plan to record and repair deficiencies in security-related equipment.			
Metric 10.4 – Maintenance Personnel Surety	The facility has procedures to verify the identity and each occurrence of contractor personnel who perform inspection, testing, and maintenance of security equipment (other than resident contractors who are included in the personnel surety program in RBPS 12).			

RBPS 11 – Training

RBPS 11 – Training - Ensure proper security training, exercises, and drills of facility personnel

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 11 – Training details the performance standards related to security and response training, exercises, and drills. By providing proper security training, exercises and drills, a facility enables its personnel to be better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. Well-trained personnel who practice how to react will be more effective at detecting and delaying intruders and provide increased measures of deterrence against unauthorized acts.

A strong training program typically includes not only personnel-specific exercises and drills, but also joint activities involving both facility personnel and law enforcement and first responders. Including law enforcement and first responders in training, exercises, and drills improves responder understanding of the layout and hazards associated with the facility while strengthening relationships with the community.

Security Measures and Considerations for Training

As one means to comply with RBPS 11, a facility should consider a Security Awareness and Training Program (SATP) commensurate with its level of risk. An SATP is a pre-defined and documented set of training activities that focus on relevant security related issues for the facility and enhance the overall security awareness of facility employees. A comprehensive SATP typically applies to all levels of facility personnel, including executives, management, operational, and technical employees. Objectives of an SATP may include validating plans, policies and procedures; and ensuring that personnel are familiar with alert, notification, deployment and other related security procedures. Typical components of a comprehensive Security Awareness and Training Program may include:

a. **Training –** Hands-on activities, seminars, orientations, workshops, on-line or interactive programs, briefings and lectures that focus on relevant security related issues for the facility.

b. **Exercises –** A pre-defined and documented set of scheduled activities that represent a realistic rehearsal or simulation of an emergency to promote preparedness, improve the response capability of individuals, and validate plans policies and procedures. Examples include tabletop exercises, functional exercises and full-scale exercises.

c. **Drills –** Drills are a sub-set or type of exercise focused on a single specific operation or function. Drills can be used to provide training with new equipment, develop new policies or procedures, or practice and maintain current skills.

d. **Tests –** Testing is the technique of demonstrating the correct operation of all equipment, procedures, processes and systems that support the security infrastructure. Tests could be static tests, dynamic tests or functional tests.

e. **Joint Initiatives –** Joint initiatives are training, exercises, or drills that involve the participation of organizations or entities outside of the facility, such as law enforcement or first responders, in conjunction with facility personnel.

Security Measures

Training

Regularly scheduled training should be considered to assure the readiness of all facility personnel. Training plans are developed and implemented to prepare individuals and groups (i.e. protective forces) to accomplish certain tasks, using selected equipment, under specific scenarios. Training may include hands-on activities, seminars, orientations, workshops, on-line or interactive programs, briefings and lectures.

The length of the training and the depth of the coverage of the information provided and discussed will vary based on the audience and method of training selected. Typically, if the audience is designated security personnel, details of security procedures, operations, communications, etc., warrants extended discussion. Awareness training for the entire workforce might include topics such as incident identification and notification.

Exercises

Exercises are conducted for the purpose of validating elements, both individually and collectively, of a facility's security posture and response capability. An exercise should be a realistic rehearsal or simulation of an emergency, in which individuals and organizations demonstrate the tasks that would be expected of them in a real emergency. Exercises should provide emergency simulations that promote preparedness, improve the response capability of individuals and organizations, validate plans, policies, procedures and systems, and determine the effectiveness of the command, control and communication functions and event-scene activities. Exercises may vary in size and complexity to achieve their respective purposes. Three typical types of exercises that a facility may want to consider including as part of an SATP are as follows:

1. **Tabletop Exercises** – simulate an emergency situation in an informal, stress-free environment. They are designed to elicit constructive discussion as participants examine and resolve problems based on existing plans. There is minimal attempt at simulation, no utilization of equipment or deployment of resources, and no time pressures. The success of these exercises is largely determined by group participation in the identification of problem areas. They provide an excellent format to use in familiarizing newly assigned/appointed security personnel and senior security officials with established or emerging concepts and or plans, policies, procedures, systems and facilities.

2. **Functional Exercises** – are fully simulated interactive exercises. They validate the capability of a group (i.e. protective force) or facility to respond to a simulated event testing one or more procedures and/or function of the facility's security plan. Functional exercises focus on policies, procedures, roles and responsibilities of single or multiple security functions before, during or after a security related event.

3. **Full-Scale Exercises** – simulate an actual security event. They are field exercises designed to evaluate the operational capabilities of the facility's physical and procedural security measures in a highly stressful environment. Typically, a full-scale exercise is an activity involving multiple parties having responsibility in the SSP for responding to a security-related event who participate in a pre-planned event where the entire SSP is rehearsed with respect to a security-related scenario. Full scale exercises involve personnel and the equipment they would use both in central control/coordinating locations and in the field.

The evaluation of an exercise should identify systemic weaknesses and suggest corrective actions that will enhance facility preparedness and response. Following an exercise, a comprehensive debriefing and after-action report are typically useful. Facilities performing such reviews may want to collect data for incorporation into a remedial action plan that provides input for annual revisions.

Drills

Drills are a coordinated, supervised activity normally used to exercise a single specific operation or function. Drills are also used to provide training with new equipment, to develop new policies or procedures, or to practice and maintain current skills.

Tests

Testing is the technique of demonstrating the correct operation of all equipment, procedures, processes and systems that support the security infrastructure. The testing process validates that the equipment and systems conform to specifications and operate in the real world environments and that procedures and processes are viable. Testing is used as the verification and validation technique to confirm that backup equipment and systems closely approximate the operations of the primary equipment and systems. Based on the measures and benchmarks desired, there are a variety of methods that can be used to test the functionality of backup environments, such as:

1. **Static Tests** – determine if all essential components of the equipment and systems are in place and meet the specification and design requirements of the facility.

2. **Dynamic Tests** – verify that all of the required equipment and systems function independently of each other, function in consort with each other and satisfy the operational requirements of the organization.

3. **Functional Tests** – verify that the procedures for operating the equipment and systems in the backup environment are correct. This testing assures that when trained and qualified personnel are required to utilize the backup equipment and systems, the instructions for operations are clear and complete.

Joint Initiatives

Joint initiatives are activities that afford the facility with the opportunity to participate in joint organization/agency (e.g., facility and local law enforcement) exercises to rehearse and exercise coordinated security related procedures.

Security Considerations

Tailoring Training Requirements

To maximize the benefit of a security awareness and training program, a facility may want to tailor training topics to specific classes of employees, as not all facility employees need the same level of training. For example, detailed training on security procedures, operating security equipment, security response protocols, and security laws and regulations may not be worthwhile for employees who do not have specific security responsibilities. Conversely, certain training topics such as incident identification and notification are beneficial for the entire workforce. Table 13 below provides examples of recommended training topics and the individuals within the organization who are most likely to benefit from that training.

Table 13: Suggested Training Topics

Training Topic	SSO/Asst SSO	Personnel with Security Responsibilities	All Remaining Employees
Security Laws and Regulations	XX		
Threats	XX		
Security Organization/Duties and Responsibilities	XX		

Table 13: Suggested Training Topics			
Training Topic	**SSO/Asst SSO**	**Personnel with Security Responsibilities**	**All Remaining Employees**
CSAT Components ▪ Top Screen ▪ Security Vulnerability Assessment (SVA) ▪ SSP ▪ Personnel Screening Database	XX		
Security Measures and Management of SSPs	XX		
Requirements for SSP	XX		
Drills and Training	XX		
Inspections and Screening	XX		
Recordkeeping	XX		
Knowledge of current security threats and patterns	XX	XX	
Recognition and detection of dangerous substances and devices ▪ Recognizing explosive materials ▪ Recognizing explosive devices ▪ Improvised explosives (e.g., using industrial materials) ▪ VBIEDs ▪ Hand-carried weapons ▪ Surveillance devices (e.g., camera phones	XX	XX	XX
Recognition of suspicious behavior	XX	XX	XX
Techniques used to circumvent security measures	XX	XX	XX
Crowd and traffic management and control techniques	XX	XX	
Security related communications	XX	XX	
Knowledge of emergency procedures, contingency plans, and crisis management plans	XX	XX	
CVI certification	XX	XX	
Operation of security equipment and systems	XX	XX	
Testing, calibration, and maintenance of security equipment and systems	XX	XX	
Relevant provisions of the SSP	XX	XX	XX
Methods of physical screening of persons and personal effects	XX	XX	
The meaning and the consequential requirements of the different DHS Threat Levels in general	XX	XX	XX

Frequency of Training, Drills, and Exercises. How frequently a facility chooses to conduct training, drills, and exercises likely will depend on a variety of factors. Such factors include the facility's risk tier, the training topic, the composition of the training's target audience, and the size of the facility. Table 14 below provides some recommended frequencies for various types of training, drills, and exercises by Tier.

Table 14: Recommended Frequency (by Tier) of Sample Activities Under RBPS 11				
Activity	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Testing of alert, notification and activation procedures	Quarterly	Quarterly	Semi-annual	Semi-annual
Testing of communications capability	Quarterly	Quarterly	Semi-annual	Semi-annual

Security awareness briefing (or other means of refresher for the entire workforce) and pre-employment for all new or temporary workers	Annual	Annual	Annual	Annual
Training for protective force personnel	Quarterly	Quarterly	Semi-annual	Annual
Training for management personnel	Annual	Annual	Annual	Annual
Drills	Semi-annual	Annual	Annual	Annual
Tabletop exercise	Every 2 years	Every 3 years	N/A	N/A
Functional exercise	Annual	Annual	N/A	N/A
Full scale exercise (with law enforcement and first responders)	Every 2 years	Every 3 years	N/A	N/A

Recordkeeping for Training

Pursuant to 6 CFR § 27.255(a)(1), a covered facility must keep records of the date, location, time of day, and duration of each training session, a description of the training, the name and qualifications of the instructor, a list of the attendees which includes a signature of each attendee and at least one other unique identifier for each attendee, and the results of any evaluation or training. Accordingly, when developing Security Awareness and Training Program, a facility may wish to consider how to best incorporate these recordkeeping functions.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 15: RBPS Metrics – RBPS 11 – Training

RBPS 11 - Training - Ensure proper security training, exercises, and drills of facility personnel

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	The facility has a security awareness and training program for all facility personnel that includes drills and exercises designed to test and improve performance of aspects of the Site Security Plan and its supporting implementing procedures.			
Metric 11.1 – Security Training Program for Security Personnel	The facility has a documented security awareness and training program, and a corresponding set of minimum skills and competencies for security personnel, as well as a testing program through which security personnel can demonstrate their ability to perform their security-related tasks in a reliable and effective manner. A typical training program will include features such as: • Training on items such as recognition of a security incident; reporting a security incident; emergency procedures; operations of security equipment. • Training is held on a regular (e.g., quarterly) basis for security personnel. • Objectives are established for each element of the training plan. • Training records are maintained in accordance with 6 CFR § 27.255(a)(1).			
Metric 11.2 – Security Training Program for	The facility has a documented security awareness and training program for employees and resident contractors without direct security responsibilities, and a testing program through which these employees and resident contractors can demonstrate their understanding of their roles in security. A typical training program will include features such as: • Training on items such as recognition of a security incident; reporting a security incident; emergency procedures;			

Table 15: RBPS Metrics – RBPS 11 – Training				
RBPS 11 – Training - Ensure proper security training, exercises, and drills of facility personnel				
Non-Security Personnel	operations of security equipment. • Training is held on a regular (e.g., annual) basis for employees and resident contractors without direct security responsibilities. • Objectives are established for each element of the training plan. • Training records are maintained in accordance with 6 CFR § 27.255(a)(1).			
Metric 11.3 – Drills and Exercises	• The facility plans and conducts security drills and exercises on a periodic basis which are documented and reviewed for lessons learned. Typical drills and exercises performed by the facility, and the corresponding frequency.	• The facility plans and conducts security drills and exercises on a periodic basis which are documented and reviewed for lessons learned. Typical drills and exercises performed by the facility, and the corresponding frequency.	• The facility plans and conducts security drills and exercises on a periodic basis which are documented and reviewed for lessons learned. Typical drills and exercises performed by the facility, and the corresponding frequency.	• The facility plans and conducts security drills and exercises on a periodic basis which are documented and reviewed for lessons learned. Typical drills and exercises performed by a facility, and the corresponding frequency, may include.

RBPS 12 – Personnel Surety

RBPS 12 - Personnel Surety - Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,
(i) measures designed to verify and validate identity
(ii) measures designed to check criminal history
(iii) measures designed to verify and validate legal authorization to work
(iv) measures designed to identify people with terrorist ties

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

Personnel surety is a key component of a successful chemical facility security program. Measures and aspects of a successful personnel surety program should build on the in-place corporate programs, as applicable. A successful personnel surety program can significantly improve a facility's capability to deter, detect, and defend against insider threats or covert attacks. RBPS 12 – Personnel Surety - establishes performance standards focused on this critical area, and addresses the need for a high-risk chemical facility to ensure that individuals allowed on-site have suitable backgrounds for their level of access.

Important aspects of implementing a personnel surety program typically include the performance of appropriate background checks, ensuring appropriate credentials, and procedures for how approval denial of access is determined.

Security Measures and Considerations for Personnel Surety

Security Measures

The primary means for satisfying the personnel surety performance standards is through the implementation of an appropriate background check program.

Background Checks

It is important to note that the use of background checks in the context of RBPS 12 is not intended to alter, limit or conflict with other federal, state or local laws and rules (see 6 CFR § 27.405(b) and 72 Fed. Reg. 17719, 17727), including those protecting workers' or applicants' rights. Similarly, background checks under RBPS 12 are not intended to be used by facilities to inappropriately or unlawfully discriminate or retaliate against employees or applicants.

Applicable Threat Scenarios

When determining what protective measures to apply to meet the Personnel Surety performance standards, a facility might consider the following potential attack scenarios:

- Assault Team
- Sabotage
- Theft/Diversion
- VBIED

In the context of CFATS RBPS 12, a background check is the process of acquiring information on an individual regarding the appropriateness of an individual for employment, for access to restricted areas, or for other activities that involve access to a restricted area or critical asset at a high-risk chemical facility. Background checks can range from simple employment screening (i.e., using public or commercially available records and investigation to confirm or disprove the accuracy of an applicant's resume) to comprehensive investigations that consider prior criminal activity, immigration status, credit checks, potential terrorist ties, and other more in-depth analysis.

Under 6 CFR § 27.230(a)(12), facilities are required to address four types of background checks on facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets:

1. Measures designed to verify and validate identity. This typically involves a social security/name trace search which reveals names associated with a social security number, past and present addresses, and fraudulent use of social security numbers. Results may also be used to cross-reference addresses supplied by the applicant to ensure the integrity of the information on the job application or resume.
2. Measures designed to check criminal history. This typically involves a search of publicly or commercially available databases, such as county, state and/or federal criminal record repositories for jurisdictions in which an individual has worked or resided. A typical criminal history search would uncover any criminal charges, outstanding warrants, dates, sentencing and disposition, for felonies and/or misdemeanors. In conducting or evaluating such a search, a facility may wish to consult the federally established list of disqualifying

crimes applicable to hazmat drivers and transportation workers at ports (see 49 CFR § 1572.103).

A second type of search that often is used to check criminal history is a national criminal scan. The national scan serves as a supplement to Criminal History Searches by searching to identify criminal activity in jurisdictions outside of current and previous residence and employment geographical locations.

3. Measures designed to verify and validate legal authorization to work. The standard way to validate legal authorization to work is through the filing of a U.S. Citizenship and Immigration Services (USCIS) Form I-9: Employment Eligibility Verification or through DHS's E-Verify program.

4. Measures designed to identify people with terrorist ties. Because information regarding terrorist ties is not publicly available, the Department is developing a system through which regulated facilities will be able to have relevant individuals screened by DHS through the Terrorist Screening Database (TSDB).

In addition to the four required types of checks, facilities may want to consider additional voluntary checks for their employees. Table 16, below, provides a list of activities that a facility may wish to consider as part of the background check process.

Table 16: Examples of Background Check Options

Background Check Contents	• Verification of social security number consistent with any applicable law.[12] • Name and address of each employer and the period employed providing information on job title. • A search of federal, state, and county criminal records in all jurisdictions in which the individual has worked or resided during the previous seven (7) years, including all geographical areas listed on the application, resume, and the social security number address verification report. The records search includes federal, state, county (or equivalent) felony and misdemeanor convictions, deferred adjudication, pleas of no contest, and unresolved indictments or other charges of crimes or offenses, except to the extent consideration of any such categories are prohibited by applicable law. Minor traffic offenses are not generally relevant; however, DWI/DUI may be relevant. • For employees whose job responsibilities involve operating motor vehicles - Information from the Department of Motor Vehicles in, but not limited to, the geographic areas listed on the application, resume, or social security number and address verification in order to reveal violations and convictions. • E-Verify or USCIS Form I-9. • Screening for terrorist ties through the Terrorist Screening Database.

There are a variety of methods through which a facility or corporation can conduct background checks, such as hiring personal investigators, or using one of many commercial websites which will perform specific searches for a fee. Corporations or facilities also can choose to perform the

[12] Facilities may wish to consider using the Social Security Number Verification System (SSNVS), provided by the Social Security Administration (SSA) to all employers, to verify that employee names and social security numbers match the SSA's records..

searches on their own as many records, such as criminal records, are available to the public for a small fee.

DHS views the background check process as one of the many pieces of the Site Security Plan. Once the facility receives the Letter of Authorization under 6 CFR § 27.245 denoting preliminary approval of the Site Security Plan, the facility should then proceed with all necessary background checks, if it has not done so already.

Special Laws Applying to Background Checks

Because of the potential sensitivity of the information uncovered, employment screening is subject to a set of laws and regulations to protect individuals in the event of misuse of data or fraud. Laws that may apply, depending on the type of background checks conducted, include the Fair Credit Reporting Act and the Driver's Privacy Protection Act. When conducting background checks, a corporation or facility should ensure that it is complying with all applicable laws, including applicable State regulations. The facility or operator may not necessarily be responsible for the compliance of contractors. The contractor may be required by contract or under law to meet background check requirements. By virtue of the contractor relationship, the corporation or facility may not know or receive results except for notice that the contractor passed.

Redress

The CFATS rule provides specific administrative adjudication and appeal procedures for any individual receiving a negative determination under 6 CFR § 27.230(a)(12)(iv) (identification of persons with terrorist ties) in connection with RBPS 12. Covered chemical facilities (or their owners or parent companies) should consider adopting a vigorous internal redress process for adversely affected applicants and personnel, including an appeal and waiver process similar to the system established for hazmat drivers and transportation workers at ports (see 49 CFR 1515).

Such an internal appeal process would be designed to provide an applicant or personnel with the opportunity to show that he or she does not have a disqualifying conviction, by correcting outdated underlying court records or proving mistaken identity.

An internal waiver process would be designed to provide an applicant or personnel with the opportunity to be hired or continue employment by demonstrating rehabilitation or facts surrounding a conviction that mitigate security concerns. Covered facilities (or their owner or parent company) should consider permitting an applicant or personnel to submit information pertaining to any of the following:

- Circumstances of the disqualifying offense;
- Restitution made;
- Letters of reference from clergy, employers, probation/parole officers; and
- Other factors the individual believes bear on his or her good character.

Such an internal redress process could be incorporated into the disciplinary procedures already used by the facility or company as part of its management/labor relations.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 17: RBPS Metrics – RBPS 12 – Personnel Surety

RBPS 12 - Personnel Surety - Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,
(i) measures designed to verify and validate identity
(ii) measures designed to check criminal history
(iii) measures designed to verify and validate legal authorization to work
(iv) measures designed to identify people with terrorist ties

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	All individuals (e.g., employees, contractors, visitors) who have unescorted access to critical or restricted areas or critical assets have appropriate background checks successfully completed.			
Metric 12.1 – New/Prospective Employees	All new/prospective employees and contractors who have unescorted access to critical or restricted areas have appropriate background checks. Access to restricted areas or critical assets are allowed after appropriate background checks have been successfully completed.			
Metric 12.2 – Existing Employees	All existing employees who have unescorted access to critical or restricted areas undergo background investigations in an expedited but reasonable period from the date of the preliminary approval of the Site Security Plan. Access is allowed following successful background screening. Investigations are repeated for all individuals in regular intervals thereafter.			All existing employees who have unescorted access to critical or restricted areas undergo background investigations in an expedited but reasonable period from the date of the preliminary approval of the Site Security Plan.
Metric 12.3 – Contents of Background Checks	The background checks are conducted in accordance with requirements established by the corporation, facility, or SSO. A contractor's employer could be the responsible entity, and a corporation or facility may require background checks as a condition to access.			
Metric 12.4 – Terrorist Screening	Processes are in place to allow for DHS to screen employees and contractors who have unescorted access to critical or restricted areas against the Terrorist Screening Database.			
Metric 12.4 – Audit	The background check program is audited regularly.		N/A	

RBPS 13 – Elevated Threats

RBPS 13 – Elevated Threats - Escalate the level of protective measures for periods of elevated threat

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

The ability to escalate the levels of security measures for periods of elevated threat provide a facility with the capacity to increase security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. By maintaining the ability to increase security measures, the facility does not have to expend time and resources on more vigorous security measures unless and until warranted.

The "Elevated Threats" RBPS addresses the need to escalate the level of protective measures for periods of elevated threat designated by DHS. The purpose of the RBPS is to enhance facility and operational security, while reducing the likelihood of a successful attack, through the implementation of scalable security measures and actions in response to changes in the Homeland Security Advisory System (HSAS) threat levels. The simplest way for a facility to meet the standards sought by RBPS 13 is to have a set of documented and implementable security procedures that provide for a change in the facility's security posture based on an elevated HSAS threat level. Properly responding to and implementing appropriate security measures in response to different threat levels significantly improves a facility's capability to "Deter, Detect and Delay" a threat (see RBPS 4), greatly reducing the likelihood of a successful attack during a period of elevated threat.

Security Measures and Considerations for Elevated Threats

Security Measures

Designing appropriate security measures for periods of elevated threat typically involves both the awareness of a period of elevated threat, and the identification of security measures tailored to the elevated threat.

Awareness of an Elevated Threat Level

DHS and its Federal security partners use a variety of mechanisms to inform the public of potential threats. The primary means of informing the public of an elevated threat is the Homeland Security Advisory System color-coded Threat Level System. Facilities will typically tie increased security measures for elevated threats to an increase in the HSAS threat level. In addition, targeted threat information is made available to the public in the form of Homeland Security Threat Advisories and Homeland Security Information Bulletins.

Color-coded Threat Level System

The Color-coded Threat Level System is used by the Federal government to communicate with public safety officials and the public at-large through a threat-based, color-coded system. This system informs economic sectors or geographic regions that they may be facing an elevated threat, thus allowing them to implement additional protective measures to reduce the likelihood or impact of an attack. DHS recognizes that raising the threat condition has economic, physical, and psychological effects on the nation, so only does so when specific threat information calls for such an increase. The five color-codes and their meanings are as follows:

1. **Low Condition (GREEN)** - this condition is declared when there is a low risk of terrorist attacks.
2. **Guarded Condition (BLUE)** - this condition is declared when there is a general risk of terrorist attacks.
3. **Elevated Condition (YELLOW)** - an Elevated Condition is declared when there is a significant risk of terrorist attacks.
4. **High Condition (ORANGE)** - a High Condition is declared when there is a high-risk of terrorist attacks.
5. **Severe Condition (RED)** - a Severe Condition reflects a severe risk of terrorist attacks.

The sample security measures in this guidance document are based upon a YELLOW threat level. Accordingly, for purposes of this RBPS, an ORANGE or RED threat level is considered an elevated threat level.

Homeland Security Threat Advisories

Homeland Security Threat Advisories contain actionable information about an incident involving, or a threat targeting, critical national networks, infrastructures or assets. Often, these threat

advisories also suggest a change in readiness posture, protective actions, or other response in light of the actionable information. This category includes products formerly named alerts, advisories, and sector notifications. Advisories are targeted to Federal, state, and local governments, private sector organizations, and international partners.

Homeland Security Information Bulletins

Homeland Security Information Bulletins communicate information of interest to the nation's critical infrastructures that may not meet the timeliness, specificity, or significance thresholds of threat advisories or other warning messages. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to Federal, state, and local governments, private sector organizations, and international partners.

Sample Security Measures for an Elevated Threat Level

A High Condition (ORANGE) is declared when there is a high-risk of terrorist attacks. In addition to the measures and procedures in place as part of the facility's steady-state protective posture, a high-risk chemical facility may want to consider implementing the following measures when the threat level is elevated to ORANGE:

- Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations
- Taking additional precautions at public events held on-site and possibly considering alternative venues or even cancellation
- Preparing to execute contingency procedures, such as moving to an alternate facility or dispersing their workforce
- Restricting threatened facility access to essential personnel only
- Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources
- Additional barriers at vehicle access points and around critical process units to control traffic and increase standoff distances
- Additional illumination for remote areas
- Decrease the number of personnel authorized to be on-site
- Extend physical protection of vulnerable points, including off-site critical facilities
- Increased frequency of perimeter patrols
- Increased security force allocations
- Increased railcar inspections
- Increased personnel and vehicle screening inspections
- Mandatory visitor escorts
- Minimize the number of gates in use
- Off-site mail handling
- Parking restrictions
- Postpone projects and activities where high-risk chemicals are more exposed or vulnerable

- Real-time reporting capability between the security control center and the main process control center
- Reinforced barriers at remote or unused gates

A Severe Condition (RED) reflects a severe risk of terrorist attacks. In addition to the protective measures taken under the ORANGE threat level, a high-risk chemical facility may want to consider implementing the following measures when the threat level is elevated to RED:

- Increasing or redirecting personnel to address critical emergency needs
- Decrease the number of personnel on-site to "essential" personnel only
- Night vision devices for security force
- Constant perimeter patrols
- Maximum security force staffing
- 100% railcar inspections
- 100% personnel and vehicle screening inspections
- No visitors allowed on-site
- No parking on-site (except vehicles always kept inside the restricted area)
- Lock down the control center to deny access to unauthorized personnel
- May have arrangements in place to secure armed response capability utilizing any combination of proprietary, contract, local, state and/or federal resources where safety at the facility is not compromised

Security Considerations

Length of Period of Elevated Threat Level

The length of an elevated threat level period is not predetermined, but rather is based on the specific threat environment that causes the elevation of the threat level. Accordingly, there is the possibility that an elevated threat level may last for a significant period of time (e.g., weeks or months). In the case of an extended period of elevated threat, it may not be feasible for a facility to maintain some of the measures it chooses to implement for a brief period of elevated threat (e.g., limiting facility access to only critical personnel; hiring armed guards). Accordingly, when planning for the potential of having to increase its security posture based on an elevated threat level, a facility may want to develop options not only for rapidly implementing an increased security posture, but also for migrating from a short term elevated security posture to a longer term, more economical elevated security posture.

Layered Security

Completely adequate protection is rarely achievable solely through implementing different security measures for changes in the HSAS threat level. Rather, an adequate security solution typically depends upon the use of multiple countermeasures providing "layers of security" that protect critical assets from malevolent acts. This includes not only the layering of multiple physical protective measures, but also the effective integration of physical protective measures with

procedural security measures, including procedures in place before an incident and those employed in response to an incident.

Availability of Personnel During Periods of Elevated Threat

Plans for dealing with periods of elevated threat often will call for increased activity from for certain individuals such as security personnel, local law enforcement, and other first responder services. However, it is not unusual for the same outside security personnel, local law enforcement, or other similar individuals to be part of the response plans for multiple locations, or to have other responsibilities during periods of elevated threat. As a result, a plan that worked during exercises may be ineffectual during an actual event. Accordingly, when planning for elevated threat periods, it is important to consider whether or not a specific individual identified in the plan has been assigned other responsibilities that may impact their ability to perform his or her identified duties during a period of elevated threat that is not limited to a specific facility.

Additional Resources on Responding to Elevated Threat Levels

Additional information on responding to elevated threat levels can be found on-line in the following locations:

- Department of Homeland Security: *Homeland Security Advisory System* (www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm)
- Ready.gov (www.ready.gov)
- National Apartment Association: *Security Measures Checklist* (www.naahq.org/NR/rdonlyres/6A82AB7E-2A5A-4FCC-9CEB-0EF1DD5C7B54/0/Security_Measures_Checklist.pdf)
- *Threat Advisory System Response Guideline, Considerations and Potential Actions in Response to the Department of Homeland Security Advisory System*, ASIS International, 2004 (www.asisonline.org/guidelines/guidelinesthreat.pdf)

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 18: RBPS Metrics – RBPS 13 – Elevated Threats

RBPS 13 - Elevated Threats - Escalate the level of protective measures for periods of elevated threat				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has a documented process for rapidly implementing an increased security posture in response to the elevation of the DHS HSAS threat level and has the ability to carry out that process in a timely manner.			

Table 18: RBPS Metrics – RBPS 13 – Elevated Threats				
RBPS 13 - Elevated Threats - Escalate the level of protective measures for periods of elevated threat				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 13.1 – Procedures	The facility has a written process and procedures for implementing security measures and increasing their security posture during periods of elevated threat to levels commensurate with the elevated threat. These security measures are specified and described in the Site Security Plan (SSP) and tied to the HSAS threat level established by DHS.			
Metric 13.2 – Time Limits	The facility can achieve the security measures associated with each respective increased HSAS threat level within 8 hours while maintaining the measures already in use during normal operating periods.	The facility can achieve the security measures associated with each respective increased HSAS threat level within 12 hours while maintaining the measures already in use during normal operating periods.		The facility can achieve the security measures associated with each respective increased HSAS threat level within 24 hours while maintaining the measures already in use during normal operating periods.

RBPS 14 – Specific Threats, Vulnerabilities, or Risks

RBPS 14 - Specific Threats, Vulnerabilities, or Risks - Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

A particular high-risk chemical facility may face threats or vulnerabilities that were not identified in the facility's SVA. In some instances, new information about a threat, vulnerability, risk or a new situation or information may come to the attention of the facility, the Department, or State or local authorities with responsibility for security. Addressing these previously unidentified, unrecognized and/or specific facility threats, vulnerabilities or risks is imperative to maintaining the security of the facility.

The purpose of the RBPS is to enhance facility and operational security, while reducing the likelihood of a successful attack, through the implementation of scalable security measures and actions in response to identified facility-specific threats, vulnerabilities or risks. Essentially, CFATS is requiring that any high-risk chemical facility address any and all threats, vulnerabilities and risks specific to that facility, as identified by the Assistant Secretary, in order to decrease the likelihood of a successful attack on its facility, personnel, products or community.

Security Measures and Considerations for Specific Threats, Vulnerabilities, or Risks

Unless notified by DHS of threats, vulnerabilities, or risks specific to the facility, a facility need not implement any measures to be in compliance with RBPS 14. Should a specific threat, vulnerability, or risk be identified, DHS can at that time work with the facility in identifying appropriate measures, procedures, or other activities that the facility could use to address the identified threat, vulnerability, or risk.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 19: RBPS Metrics – RBPS 14 –Specific Threats, Vulnerabilities, or Risks

RBPS 14 - Specific Threats, Vulnerabilities, or Risks - Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has implemented security measures that address any and all specific threats, vulnerabilities or risks identified for the facility by the Assistant Secretary.			
Metric 14.1 – RBPSs	Measures implemented to address the specific threats, vulnerabilities or risks meet the metrics for all other applicable RBPS for the facility.			
Metric 14.2 – Documentation in SSP	Measures implemented to address the specific threats, vulnerabilities or risk are documented in the SSP.			
Metric 14.3 – Training	All applicable employees have been trained on the measures implemented to address the specific threats, vulnerabilities or risk in accordance with the facility security awareness and training program.			

RBPS 15 – Reporting of Significant Security Incidents

RBPS 15 – Reporting of Significant Security Incidents - Report significant security incidents to the Department and to local law enforcement officials

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 15 – Reporting of Significant Security Incidents addresses the importance for high-risk chemical facilities to promptly and adequately report all significant security incidents to the appropriate facility personnel, local law enforcement entities, and DHS. Pursuant to 6 CFR §27.230(a)(15), a facility is required to report significant security incidents to the Department and to local law enforcement officials. To facilitate the accomplishment of this responsibility, a facility would benefit from the establishment of protocols governing reporting of an incident to facility security and up through the security chain of command of the facility and the company that owns or operates the facility. Protocols for determining whether or not a security incident is significant and warrants informing DHS and/or local law enforcement, as well as the process for actually reporting the incident, also would be beneficial to a facility.

Security Measures and Considerations for Reporting of Significant Security Incidents

Security Measures

Complying with RBPS 15 typically involves four basic steps: (1) identifying a security incident; (2) reporting it to facility security; (3) determining whether or not the incident is a "significant security incident;" and, if it is a significant security incident, (4) reporting it to DHS and local law enforcement.

Identifying and reporting to facility security a security incident. The easiest way for a facility to prepare its employees to identify and report security incidents is to clearly articulate to its employees, and especially to its security staff, how to identify a security incident and how to respond to it, including to whom to report the incident. This can be achieved, for example, by establishing clear protocols regarding security incidents, and training of facility employees on these protocols as part of a facility security awareness and training program.

Determining if an incident is a "significant" security incident. A broad spectrum of events may be considered a security incident, ranging from trespassing, vandalism, and petty theft, to cyber attacks, bomb threats, and armed attacks. Determining whether or not an incident is serious enough to be considered "significant" and thus reported to DHS and local law enforcement is generally within the discretion of the facility, and typically will be determined by the facility security officer or other senior manager. "Significant security incidents" likely will include incidents that arise based on an intentional threat (i.e., potential attack scenarios) that attempt to or successfully circumvent a security measure and/or a metric of any RBPS, for example:

- An intentional, unauthorized, successful or unsuccessful breach of the facility's restricted area perimeter
- An intentional, unauthorized, successful or unsuccessful breach of any critical asset's restricted area perimeter
- An intentional, unauthorized, successful or unsuccessful act to either forcefully or covertly bypass, circumvent or pass through any access control point
- Any incident in the vicinity of the facility or any act against the facility that requires the facility to implement additional security measures, activate procedures, or respond to with the intent of actively deterring, detecting and/ or delaying an actual threat
- Any inventory control issues, product stewardship issues, theft or diversion of any chemical of interest or other dangerous chemical, tampering with any chemical of interest or any transportation container used to transport a chemical of interest, introduction of any foreign substance into any chemical of interest or into any transportation container carrying or used to carry a chemical of interest
- Any act of tampering with malicious intent to cause undesirable consequences through the act itself
- Any incident with malicious intent to adversely affect operations of critical cyber assets, including IT equipment used to provide security for the facility, manage processes involving chemicals of interest, or manage critical assets of the facility

Reporting an incident to DHS or local law enforcement. If a significant security incident is detected while in progress, the first call typically should be to local law enforcement and emergency responders via 911. Similarly, it is recommended that a facility report the incident immediately to local first responders via 911 if the incident has concluded but an immediate emergency response is necessary. Once the incident has concluded and any immediate resulting emergency has been dealt with, a facility should use a non-emergency number to inform local first responders (if they had not already been contacted) and the Department of Homeland Security. Within the Department of Security, incidents should be reported to the National Infrastructure Coordinating Center (NICC) at nicc@dhs.gov or (202) 282-9201. In addition to the NICC, a facility may wish to contact their local FBI Field Office, whose phone number can be found online at www.fbi.gov/contact/fo/focities.htm.

Scenario-Specific Decisions on Significance

Whether an incident is significant will depend on the specific circumstances surrounding the incident, and blanket decisions regarding whether a category of actions is or is not significant may not be the best approach. For instance, trespassing may not rise to the level of significant if the trespasser is a teenager skate-boarding on a facility parking lot, but clearly is significant if the trespasser is performing surveillance for a potential terrorist attack.

Near Misses

Simply because an attack or other incident is not carried out successfully does not mean that the incident was insignificant and should not be reported. Whether a "near miss,"—i.e., an adversarial action that was attempted but not successfully completed—is significant depends on the specific circumstances, such as the desired outcome of the attempt and the motive for the attempt. All near misses should be reviewed to determine whether or not reporting to DHS or local law enforcement is justified.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 20: RBPS Metrics – RBPS 15 – Reporting of Significant Security Incidents

RBPS 15 - Reporting of Significant Security Incidents - Report significant security incidents to the Department and to local law enforcement officials				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has a process in place to rapidly and efficiently report security incidents to the appropriate entities (e.g., corporate management, local law enforcement, DHS).			
Metric 15.1 – Reporting Procedures	The facility has written procedures and related personnel training that specifically identify the types of incidents to report, the process for reporting these incidents, to whom these incidents should be reported, and who is responsible for reporting such incidents.			
Metric 15.2 –	Any detection of a suspicious person, vehicle or device, or facility intrusion alarm triggers an immediate notification of			

Table 20: RBPS Metrics – RBPS 15 – Reporting of Significant Security Incidents				
RBPS 15 – Reporting of Significant Security Incidents - Report significant security incidents to the Department and to local law enforcement officials				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Whom to Notify	facility security personnel and, if appropriate, local law enforcement and DHS. The facility promptly communicates with authorized law enforcement and DHS subsequent to any verified loss or theft of dangerous chemicals such as chemicals of interest.			

RBPS 16 – Significant Security Incidents and Suspicious Activities

RBPS 16 - Significant Security Incidents and Suspicious Activities - Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

The "Significant Security Incidents and Suspicious Activities" RBPS addresses the need for high-risk chemical facilities to promptly and adequately identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the facility. This RBPS is complementary to RBPS 15 – Reporting of Significant Security Incidents.

Security Measures and Considerations for Significant Security Incidents and Suspicious Activities

Security Measures

As part of its responsibilities under RBPS 16, it is anticipated that a facility would undertake the following activities in regard to any significant security incidents and suspicious activities:

1. **Identify** – any process by which unusual behavior, suspicious activity and/or actual incidents are identified by the facility. This includes activities such as monitoring, inspections, alarms, patrols, and security awareness and training, all of which are addressed in greater detail in connection with other RBPSs.

2. **Investigate** – the process implemented by the facility to understand, resolve and learn from all of the circumstances, evidence and other factors surrounding a security incident or suspicious activity.

3. **Report** – the process of informing facility security and management, local law enforcement and first responders, and DHS of an incident or suspicious activity. Reports of significant security incidents are required under the regulations pursuant to RBPS 15.

4. **Maintain Records** – any processes used by the facility to keep records of security incidents or suspicious activities. Pursuant to 6 CFR §27.255 (a)(3), a facility is required to keep certain information on incidents and breaches of security for a period of at least three years. Methods of meeting this requirement are discussed in greater detail in RBPS 18 – Records.

Security Considerations

The Varied Purposes of Investigating, Reporting, and Maintaining Records

When developing protocols for identifying, investigating, reporting, and maintaining records of security incidents and suspicious activities, it is important to keep in mind that each of these activities simultaneously serves multiple purposes. For instance, proper investigation, reporting, and recordkeeping assists a facility not only in identifying whether an incident or suspicious activity truly has occurred, but also in gathering evidence for the potential prosecution of the individuals perpetrating the act, and helping to identify weaknesses or gaps in a facility's security posture that may have been exploited so that those gaps can be closed.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or

targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 21: RBPS Metrics – RBPS 16 – Significant Security Incidents and Suspicious Activities				
RBPS 16 – Significant Security Incidents and Suspicious Activities - Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has documented processes and procedures for identifying, investigating, reporting on, and maintaining records of significant security incidents and suspicious activities.			
Metric 16.1 – Investigation Procedures	The facility has written procedures, either in its SSP or elsewhere, and qualified personnel for conducting thorough investigations of significant security incidents, and thoroughly investigates security breaches and incidents, including "near misses," to determine their level of threat, vulnerabilities that were exploited, and what security upgrades, if any, are warranted to reduce the security risk.			
Metric 16.2 – Lessons Learned	Lessons learned from security incidents are disseminated to appropriate facility personnel in a timely manner in meetings, by e-mail, or as part of the on-going security awareness program depending upon the nature of the incident.			

RBPS 17 – Officials and Organization

RBPS 17 - Officials and Organization - Establish official(s) and an organization responsible for security and for compliance with these standards

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 17 – Officials and Organization concerns the identification of the individual(s) and organization(s) within a company that are responsible for facility security, including compliance with all of the RBPS. Pursuant to RBPS 17, a facility must identify at least one official, as well as the organization within the company, responsible for security and compliance with the RBPSs. The manner in which a facility structures its security organization to meet this specific RBPS is likely to depend in large part on how large or complex a facility or its ownership structure is. A larger, more complex facility is likely to have a more complex organization responsible for compliance than a smaller, lower tiered facility, and also is more likely to employ an individual whose principal job responsibility is facility security.

Security Measures and Considerations for Officials and Organization

Security Measures

DHS generally anticipates that each facility will identify either a Site Security Officer (SSO) or other individual who serves as the point of contact in regards to CFATS-related communications, as well as a facility security organization responsible for implementing the Site Security Plan at the facility. Please note that depending on the size and complexity of the corporation, as way as the risk's associated with a given facility, a facility's security organization may consist of only one or two individuals.

Site Security Officers. Around the time that the facility is notified that it must submit an SVA and SSP (i.e., after DHS informs the facility that it is in fact "high-risk"), it should consider designating an SSO or other individual responsible for compliance with the RBPSs, if it has not already done so. Potential responsibilities of the SSO (or equivalent individual) may include:

- conducting and supervising the submission of the Security Vulnerability Assessment
- preparing the initial Site Security Plan and updating it
- conducting annual internal audits
- hosting DHS inspections
- designing and documenting security training for all employees
- maintaining required records
- planning and documenting security drills
- ensuring that security equipment is properly maintained, calibrated, and tested
- understanding and maintaining a list of local emergency responders, local law enforcement and local DHS Protective Security Advisors
- responding, recording and reporting all security incidents
- for facilities where theft and diversion of COI or other dangerous chemicals is a concern, the SSO may also be responsible for ensuring material accountability and control
- ensuring notification of plant personnel regarding changes in security procedures or DHS threat level
- other activities associated with the management of facility security per 6 CFR Part 27
- understanding current security threats and patterns related to the facility

Qualifications for being an SSO (or equivalent) may include:

- Understanding the security organization of the facility
- Understanding the requirement to comply with the CFATS RBPSs
- Experience in emergency preparedness, response and planning for disasters
- Familiarity with responsibilities and functions of local, State and Federal law enforcement agencies
- Ability to recognize characteristics and behavioral patterns of persons who are likely to threaten security

The individual designated to serve as the SSO (or equivalent), and the manner in which he or she carries out their responsibilities, is likely to vary greatly by company. For example, some SSOs may be dedicated full-time to facility security, while for others security is only one of multiple responsibilities. Additionally, some SSOs may be located on-site while others may be located elsewhere (e.g., corporate headquarters). Finally, in many cases an SSO will be responsible for security at a single facility; in other cases, an individual SSO may be responsible for security at multiple facilities.

Facility Security Organizations. In addition to designating an SSO or equivalent individual, facilities are required to identify the organization responsible for facility compliance with the RBPSs. The size and structure of the security organization is likely to vary based on a variety of factors, such as size of the facility, complexity of security at the facility, the security risks associated with the facility, and whether or not the facility's parent company has multiple facilities that are regulated high-risk facilities.

As part of many facility security organizations, a facility is likely to designate security responsibilities to various individuals. These may or may not include the following individuals:

- The owner/operator of the facility or his designate
- A Site Security Officer (SSO)
- A Cyber Security Officer (this may or may not be the same individual as the SSO)
- A designated Alternate SSO
- A Corporate Security Officer who coordinates SSOs across facilities
- The Facility Plant Manager

Potential security responsibilities for these other individuals could include the following:

- Owner/operator of the facility: the role of the owner/operator is to define a security organizational structure in writing that identifies specific security duties and responsibilities.
- Cyber Security Officer: the role of the Cyber Security Officer is to oversee cyber security issues at the facility.
- Alternate SSO: the role of the alternate SSO is to be able to function in place of the SSO should circumstances or the owner/operate dictate. Responsibilities assigned to the SSO, become the responsibility of the Alternate SSO in the SSO's absence.
- Corporate Security Officer (CSO): the role of the CSO is to coordinate security at a corporate level if more than one facility is subject to CFATS.
- Facility Plant Manager: the role of the facility plant manager is to ensure cooperation of facility personnel with the requirements of the SSP and CFATS, such as:
    - Coordinating training in security awareness and other security issues for facility personnel not designated to serve on the security organization
    - Ensuring that security considerations are acknowledged and implemented throughout the facility
    - Being cognizant of security risks and issues related to the facility, the community and the current threat level
    - Ensuring that adequate space and resources are available for the security organization

- Ensuring that employees can report and question security procedures without fear of retribution

A comparison of some possible roles and responsibilities of the SSO/Alternate SSO and other individuals in the facility security organization is contained in Table 22 below.

Table 22: Typical Roles and Responsibilities of Site Security Officer and Other members of Facility Security Organization

Individual	Roles and Responsibilities
SSO/Asst SSO	• Ensuring that individuals assigned to the security organization discharge their duties appropriately. • Conducting and supervising the submission of the Security Vulnerability Assessment (SVA) or an Alternate Security Program (for Tier 4 facilities). • Preparing the initial Site Security Plan (SSP) and updating it . • Conducting annual internal audits. • Designing and documenting security training for all employees to include security awareness of all personnel. • Maintaining required records. • Planning and documenting security drills. • Ensuring that security equipment is properly maintained, calibrated, and tested. • Understanding and maintaining a list of local emergency responders, local law enforcement and local DHS Protective Security Advisors. • Responding to, recording, and reporting all security incidents. • Notifying plant personnel regarding changes in security procedures or threat level. • Other activities associated with the management of facility security. • Understanding current security threats and patterns related to the facility.
Facility Management	• Coordinating training in security awareness and other security issues for facility personnel not designated to serve on the security organization. • Ensuring that security considerations are acknowledged and implemented throughout the facility. • Being cognizant of security risks and issues related to the facility, the community and the current threat level. • Ensuring that adequate space and resources are available for the security organization. • Ensuring that employees can report and question security procedures without fear of retribution.

Security Considerations

Cyber Security Officers

If a facility has significant cyber assets, it likely will want to designate a specific cyber Security Officer to be in charge of oversight of cyber security issues at the facility. This individual may be the SSO or other individual, and may be located at the facility or elsewhere (e.g., corporate headquarters). To avoid potential conflicts of interest between systems operation and security, a facility may want to have the Cyber Security Officer be a different individual than the one who is responsible for IT management or systems administration.

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 23: RBPS Metrics – RBPS 17 – Officials and Organization				
RBPS 17 - Officials and Organization - Establish official(s) and an organization responsible for security and for compliance with these standards				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility has established an official(s) and an organization responsible for security and for compliance with the RBPSs, and has included the names, contact information, and responsibilities of such officials in the Site Security Plan.			
Metric 17.1 – Owner/Operator Responsibilities	The owner/operator is responsible for defining a security organizational structure in writing that identifies specific security duties and responsibilities.			
Metric 17.2 – Corporate Security Officer (CSO) Responsibilities	The Corporate Security Officer (CSO) is responsible for coordinating security at a corporate level when a corporation has more than one facility subject to CFATS.			
Metric 17.3 – Site Security Officer (SSO) / Assistant SSO Responsibilities	The Site Security Officer (SSO) is responsible for security at the facility, including leading the implementation of the RBPSs on a facility level. The Alternate SSO is responsible for filling in for the SSO when the SSO is unavailable.			
Metric 17.4 – Cyber Security Officer	The Cyber Security Officer is the individual designated to be in charge of oversight of cyber security issues at the facility. This individual may be the SSO or other individual, and may be located at the facility or elsewhere (e.g., corporate headquarters).			
Metric 17.5 – Facility Management Roles	The facility plant manager is responsible for ensuring cooperation of facility personnel with the requirements of the SSP and the RBPSs.			

RBPS 18 – Records

RBPS 18 - Records - Maintain appropriate records

RISK-BASED PERFORMANCE STANDARDS GUIDANCE DOCUMENT DISCLAIMER

To assist high-risk facilities in selecting and implementing appropriate protective measures and practices and to assist DHS personnel in consistently evaluating those measures and practices for purposes of the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, DHS's Infrastructure Security Compliance Division has developed this *Risk-Based Performance Standards Guidance Document*. This guidance reflects DHS's current views on certain aspects of the Risk-Based Performance Standards (RBPSs) and does not establish legally enforceable requirements for facilities subject to CFATS or impose any burdens on the covered facilities. Further, the specific security measures and practices discussed in this document are neither mandatory nor necessarily the "preferred solution" for complying with the RBPSs. Rather, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the RBPSs. Facility owners/operators have the ability to choose and implement other measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the CFATS RBPSs. For example, the Site Security Plan (SSP) for a facility that is considered high-risk solely due to the presence of a theft/diversion chemical of interest (COI) likely will not have to include the same types of security measures as a facility that is considered high-risk due to potential release hazards. Similarly, the SSP for a university or medical research facility would not be expected to include the same type or level of measures as a complex chemical manufacturing plant with multiple COIs and security issues.

RBPS 18 – Records addresses the creation, maintenance, protection, storage, and disposal of appropriate security-related records pursuant to 6 CFR § 27.255, and making these records available to DHS upon request.

Security Measures and Considerations for Records

Security Measures

Section 27.255 of CFATS requires covered facilities to keep the following records for three (3) years:

- training;
- drills and exercises;
- incidents and breaches of security;
- maintenance, calibration, and testing of security equipment;
- security threats;

- audits of Site Security Plans (including audits required under 6 CFR § 27.225(e)) and Security Vulnerability Assessments;
- letters of authorization and approval from DHS; and
- documentation identifying the results of audits and inspections conducted pursuant to 6 CFR §27.250.

The following records must be retained for at least six (6) years:

- submitted Top-Screens;
- submitted Security Vulnerability Assessments;
- submitted Site Security Plans;
- all related correspondence with the Department.

The standard embodied in RBPS 18 – to maintain appropriate records – implicitly covers creation, maintenance, protection, storage, and disposal of affected records and making such records available to DHS upon request pursuant to 6 CFR §§ 27.250(a) & 27.255(b).

1. **Creation** of records refers to the preparation of a detailed written account of a covered activity. Writing this information down or recording it electronically creates a written record of it. Back-up files, duplicates or copies should be protected and maintained or disposed of in compliance with the RBPS, 6 CFR § 27.255 and/or the CFATS provisions regarding Chemical-terrorism Vulnerability Information (CVI), 6 CFR § 27.400.

2. **Maintenance** of records refers to keeping the written or electronic records in an accessible location and ensuring they are not disposed of before the time period for their retention has elapsed. Records may be maintained in paper or electronic format. Records should be maintained where they will not be disturbed, damaged or lost.

3. **Protection** of records refers to safeguarding the written or electronic records from theft, destruction, amendment, damage, misuse or unauthorized access. This includes protecting records physically as well as ensuring that CVI records are not distributed to unauthorized users.

4. **Storage** refers to keeping records in an appropriate and accessible location. Such a location may or may not be at the facility, but should be known and accessible to facility personnel should they need to retrieve such records for a DHS inspection or audit. If records are kept locked, more than one person should be able to access the records in order to produce them for a DHS inspection/audit.

5. **Disposal** refers to the destruction of records that are no longer required to be retained by the covered facility. Some records must be retained under 6 CFR § 27.255 for 3 years and some for 6 years (see list above). After this period elapses, facilities are no longer required by CFATS to maintain these records and may choose to dispose of such records rather than continuing to store them, provided that destruction of CVI complies with 6 CFR § 27.400(k).

6. **Making records available** means that the records can be produced by the facility to which they pertain for examination and copying by DHS within a reasonable period of time. This

applies not only to records created under CFATS, but also to records necessary for security purposes kept pursuant to other Federal programs or regulations (see 6 CFR § 27.255(c)).

Security Considerations

Chemical-terrorism Vulnerability Information (CVI)

It should be noted that all records required to be created or retained under 6 CFR § 27.255, are considered CVI under 6 CFR § 27.400((b)(6) and must be protected, maintained, and marked as such unless records maintained under § 27.255(1)-(5) were created to satisfy a regulatory requirement other than 6 CFR Part 27. See 72 Fed. Reg. 17715 (April 9, 2007). For additional information on CVI, please refer to the DHS Chemical Security website (www.dhs.gov/chemicalsecurity).

RBPS Metrics

The following table provides a narrative summary of the security posture of a hypothetical facility at each tier in relation to this RBPS and some example measures, activities, and/or targets a facility may seek to achieve that could be considered compliant with the RBPS. However, a facility may choose to demonstrate compliance through other measures, activities, and/or targets, provided DHS is satisfied that the measures demonstrated meet the level of performance specified in the RBPS.

Table 24: RBPS Metrics – RBPS 18 – Records

RBPS 18 - Records - Maintain appropriate records				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Summary	The facility creates, maintains, protects, stores and makes available for inspection by DHS certain records related to its security program.			
Metric 18.1 – Training Records	The facility retains training records, in paper or electronic format, for at least 3 years. The training records include the date and location of each training session, time of day and duration of each session, a description of the training, the name and qualifications of the instructor, a list of attendees which includes each attendee's signature, and the results of any evaluation or testing.			
Metric 18.2 – Records of Drills and Exercises	The facility retains records of drills and exercises, in paper or electronic format, for at least 3 years. Such records include, for each drill or exercise, the date held, a description of the drill or exercise, a list of participants, a list of equipment (other than personal equipment) tested or employed in the exercise, the name(s) and qualifications of the exercise director, and any best practices or lessons learned which may improve the Site Security Plan.			
Metric 18.3 – Records of Security Incidents	The facility retains records of incidents and breaches of security, in paper or electronic format, for at least 3 years. Such records include the date and time of occurrence, location within the facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response.			
Metric 18.4 – Maintenance Records	The facility retains records of maintenance, calibration, and testing of security equipment, in paper or electronic format, for at least 3 years. Such records include the date and time, name and qualifications of the technician(s) doing the work, and the specific security equipment involved for each occurrence of maintenance, calibration and testing.			
Metric 18.5 – Records of Security Threats	The facility retains records of security threats, in paper or electronic format, for at least 3 years. Such records include the date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response.			
Metric 18.6 – Audit Records	The facility retains records of audits, in paper or electronic format, for at least 3 years. Such records include, for each audit of a facility's Site Security Plan or Security Vulnerability Assessment, a record of the audit, results of the audit,			

Table 24: RBPS Metrics – RBPS 18 – Records				
RBPS 18 - Records - Maintain appropriate records				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	names(s) of the person(s) who conducted the audit, and a letter certified by the covered facility stating the date the audit was conducted.			
Metric 18.7 – Letters of Authorization	The facility retains all Letters of Authorization and Approval from DHS, and documentation identifying the results of audits and inspections conducted pursuant to §27.250, in paper or electronic format, for at least 3 years.			
Metric 18.8 – Correspondence with DHS	The facility retains records of submitted Top-Screens, Security Vulnerability Assessments, Site Security Plans, and all related correspondence with the Department, in paper or electronic format, for at least 6 years.			
Metric 18.9 – ASP	The facility retains records related to an Alternative Security Program which is submitted in lieu of a Security Vulnerability Assessment (Tier 4 only) or a Site Security Plan (All Tiers) pursuant to §27.235, for at least 6 years.			

Appendix A – Acronyms

Buffer Zone Protection Plan	BZPP
Chemical Facility Anti-Terrorism Standards	CFATS
Chemical of Interest	COI
Chemical Security Assessment Tool	CSAT
Chemical-terrorism Vulnerability Information	CVI
Closed Circuit Television	CCTV
Community Hazards Emergency Response-Capability Assurance Process	CHER-CAP
Code of Federal Regulations	CFR
Continuity of Operations Plans	COOP
Corporate Security Officer	CSO
Department of Defense	DOD
Department of Homeland Security	DHS
Department of State	DOS
Distributed Control Systems	DCS
Emergency Medical Technicians	EMT
Homeland Security Advisor	HSA
Homeland Security Advisory System	HSAS
Improvised Explosive Device	IED
Industrial Control Systems	ICS
Inspection, Testing and Preventative Maintenance	ITPM
Internet Protocol	IP
Intrusion Detection System	IDS
Local Emergency Planning Committee	LEPC
Local Law Enforcement	LLE
Material Safety Data Sheet	MSDS
Process Control Systems	PCS
Protective Security Advisor	PSA
Radio Frequency Identification Device	RFID
Risk Based Performance Standard	RBPS
Safety Instrumented Systems	SIS
Screening Threshold Quantity	STQ
Security Awareness and Training Program	SATP
Security Vulnerability Assessment	SVA
Site Security Officer	SSO
Site Security Plan	SSP
Supervisory Control and Data Acquisition	SCADA
Terrorist Screening Database	TSDB
Transportation Worker Identification Card	TWIC
United States Citizenship and Immigration Services	USCIS
Vehicle Borne Improvised Explosive Device	VBIED
Virtual Private Network	VPN
Voice Over Internet Protocol	VoIP

Appendix B – RBPS Metrics by Tier

Appendix C – Security Measures and Security Considerations

Throughout this Guidance document, basic information on security measures and security considerations is provided relative to each Risk Based Performance Standard (RBPS) contained in the Chemical Facility Anti-Terrorism Standards, 6 CFR Part 27. The following is a more detailed look at various examples of (1) physical security measures; (2) cyber security measures; and (3) security procedures, policies, and plans that could be used by facilities to address the variety of security risks that they face. Included for each of these three areas is a discussion on the types of measures, procedures, policies, or plans that a facility may want to employ; considerations to have in mind when selecting which measures, procedures, policies, and plans to implement; the RBPSs that a specific measure, procedure, or policy is likely to impact; and additional online resources where more information can be found on specific related topics.

It should be noted that no single measure, policy, or procedure listed below will alone satisfy the security needs of a facility. Rather, effective facility security typically involves the successful integration of a suite of measures, procedures, and policies targeted to the unique risks each facility faces. It should also be noted that no covered facility is required to adopt any or all of the specific measures, policies or procedures discussed below in order to comply with the RBPS established by CFATS. Rather, covered chemical facilities are free to include any measures they think appropriate to demonstrate compliance with the RBPS in their Site Security Plans (SSP) under §§ 27.225(a)(2) and 27.230(a) of CFATS, provided that the Department of Homeland Security determines upon review that the SSP meets the applicable RBPS and otherwise satisfies the requirements of § 27.225.

Physical Security Measures

A wide range of physical security measures are available to help reduce the risks associated with chemical facilities. Generally speaking, physical security measures are most useful for reducing the risks of direct, physical attacks against the facility. Categories of physical security measures that a facility should consider include (1) perimeter barriers; (2) monitoring and intrusion detection systems; (3) security lighting; (4) and protective forces.

Perimeter Barriers

Perimeter barriers reduce the likelihood of unauthorized persons accessing the facility for malicious purposes such as theft, sabotage, or intentional release of chemicals of interest. By securing and monitoring the perimeter of the facility, facility personnel can more easily and effectively control who enters and leaves the facility, both on foot and in vehicles, and are better able to detect, delay, defend against, and respond to individuals or groups who seek unauthorized access to the facility. A well-secured perimeter additionally will help to deter intruders from seeking to gain access to the facility or from launching attacks from the area immediately outside a facility's perimeter.

Perimeter barriers provide both physical obstacles and psychological deterrents to unauthorized entry, delaying or preventing forced entry. Perimeter barriers can be used in a variety of ways to restrict the area perimeter and increase overall facility security, including:

- Controlling vehicular and pedestrian access
- Providing channeling to facility entry-control points
- Delaying forced entry
- Protecting critical assets

Perimeter barriers generally can be either manmade or natural.

Manmade Barriers

As the name suggests, manmade barriers are those that are manufactured synthetically by humans. Typically, manmade perimeter barriers come in three varieties: (1) human barriers, (2) vehicle barriers, and (3) walls. Common examples of all three of these varieties of barriers are contained in Table A1.

Table A1: Common Manmade Barriers

Human Barriers	Vehicle Barriers	Walls

• Barbed Wire (on the ground)
• Casehardened Chains and Locks
• Concertina Wire (on the ground)
• Fence
  - Chain Link
  - Concrete
  - Metal
  - Vinyl
  - Wood
• Gate
  - Chain Link
  - Metal
  - Wood
	• Anti-vehicle cable
	• Beam
	• Berm
	• Bollard
	• Vehicle capture net
	• Cable-beam / Cantilever
	• Casehardened Chains and Locks
	• Drop Arm (crash rated)
	• Embankment
	• Fence
	  - Concrete
	  - Metal
	  - Chain Link
	  - Vinyl
		• Brick
		• Cinder block
		• Metal
		• Poured concrete

Table A1: Common Manmade Barriers		
Human Barriers	**Vehicle Barriers**	**Walls**
	- Wood • Gate - Chain Link - Metal - Wood • Jersey Barrier/K-rail • Planter • Slalom or Serpentine Chicane • Wedge barrier	

Human Barriers

Human barriers protect critical assets by controlling pedestrian access and delaying or preventing forced entry. The typical human barrier consists of a combination of fencing and gates. Fencing is the most basic first line of deterrence and defenses.

The most commonly used manmade human barrier by industrial facilities is chain link fencing. Chain link fencing is readily available through a large variety of sources and is easily and inexpensively maintained. This type of fence provides clear visibility for security patrols, and is available in varieties that can be installed in almost any environment.

While fencing alone typically is not sufficient at high-risk facilities, its level of effectiveness can be elevated simply by adding barbed wire, razor wire, or other available toppings to increase intrusion difficulty.

Vehicle Barriers

Vehicle barriers protect critical assets by controlling vehicular access and delaying or preventing forced entry. Barriers typically are placed either along a facility's perimeter to protect it from direct penetration, or arranged in a manner to control and slow traffic as it approaches facility access points.

Vehicle barriers are often given "K Ratings" indicating the size and speed of vehicle the barrier can be expected to stop. These ratings are based the kinetic energy represented by the mass of a vehicle and its impact velocity. To be certified with a Department of State "K" rating, a barrier must demonstrate the ability to stop a 15,000 lb vehicle, with the bed of the vehicle not penetrating the barrier by more than 36 inches. The "K" ratings are:

K4	15,000 lb vehicle impacting at 30 mph
K8	15,000 lb vehicle impacting at 40 mph
K12	15,000 lb vehicle impacting at 50 mph

Additional information on DOS security measures can be obtained from the DOS Bureau of Diplomatic Security, Physical Security Program, Physical Security Division (DS/PSP/PSD).

Common manmade vehicle barriers include[13]:

- Jersey Barriers (or other Concrete Barriers): Jersey barriers, which were originally designed to serve as highway medians, are concrete barriers specifically designed to impede moving vehicles. These barriers come in a variety of forms, and are available both as pre-made sets that can be assembled at a facility, or can be cast in place with special concrete-forming equipment. Jersey barriers also are often referred to as K rails.

- Bollards: A bollard is a post made of concrete, stainless steel, aluminum, cast iron, or other durable material, that creates an aboveground obstacle. Bollards can be fixed or retractable. At the high end, bollards are constructed to completely stop most vehicles.

- Chain link gate reinforcement: Wire ropes are fastened to gates and anchored on either side of the gate. For a relatively weak gate, the reinforcement transfers the force of a vehicle impact to a more substantial anchor system. It can be used on many different gate applications.

- Cable barriers: Cable is fastened to each post with U-clamps and is periodically anchored. The barrier prevents light vehicles from crashing through a standard chain link fence. One disadvantage is that the cable can be covertly cut when installed along the outermost perimeter.

- Drum and Cable Barriers: Drums are filled with dirt, rock or concrete attached by aircraft cable to another drum or fixed object. This typically involves minimal setup time and expense. This can be a cost-effective application since empty storage drums, dirt, and rock are readily available.

- Dragnet: This consists of a chain link "net" assembly with arresting cables attached to an energy absorber that is attached to the anchor system. In the open position, the dragnet is suspended above the access road. When a vehicle hits the dragnet in the closed (dropped) position, the energy form the impact is transferred through the arresting cables to an energy absorber that brings the vehicle to a controlled stop.

- Removable nuisance barrier: A pipe driven into the ground and fastened with a coil chain is used to channel traffic and create marked isolation zones around sensitive areas, equipment, and buildings. It can be set up and removed quickly and easily.

- Guardrail: Standard highway guardrails or median barriers; cable, W-beam, or box beam guardrails are used as a perimeter barrier. They are not designed to prevent head-on penetrations but can immobilize a lightweight vehicle attempting an intrusion.

- Traffic Control Island with Vehicle Barriers: Standard guard post, with two automatic gates, a custom base, platform curb assembly with three pass-throughs, and barrier posts provide protection for security personnel stationed at vehicle entrance.

[13] http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/DesignConsiderations/CD/appd.htm

- Motorized Barricade: This refers to a steel barricade that can be deployed to close off vehicle access. Several activation options are possible, such as by remote switch or card reader.

- Hydraulic Barricade: Upon major impact, the lifting mechanism absorbs the shock. In emergency situations, a steel barricade closes off vehicle access in just one second.

- Electronic Barrier Gate: Chain link gates and turnstiles used for vehicle and personnel entrances, electronic barrier gates may be activated by remote switch, numerical code, or card reader.

- Tire-Penetrating Traffic Barrier (One-way Tire Trendles): A row of steel teeth that are unidirectional, spring-loaded, and are embedded in the road. The barrier punctures the tires of an intruding vehicle, while allowing passage of vehicles in the opposite direction.

- Portable Roadblock Tire-Puncturing Device: Hollow stainless steel spikes mounted on aluminum scissors action arms expand to stretch across a vehicle access. Anchors hold the scissors in place. The system expands to cover 21 feet and folds into a case weighing 35 pounds. When an intruding vehicle passes over the system, the spikes imbed into the vehicle's tires and detach from the aluminum frame. This opens several "tubes" which cause rapid uniform deflation and prevent the holes from sealing. Since the air loss is uniform from all times, the operator is more likely to maintain control of their vehicle. These devices are most effective against light vehicles with standard 3/4-inch thick rubber tires.

Walls

Walls are one of the most common types of barriers. Various types of walls are used for interior, as well as exterior, security boundary separation. Walls typically play an important part as visual barriers and deterrents. Additionally, depending on its structure, a wall can serve as a human barrier and/or a vehicle barrier.

While exterior walls are typically not as economical as chain link fencing, the use of exterior walls as barriers is frequently necessary. Walls provide less visibility of storage or secured areas and can be matched to the surrounding architecture and buildings. In addition, some varieties of exterior walls are less climbable and thus more secure than security fencing or other barriers that offer hand-holds.

Natural Barriers

Natural barriers can be an effective barrier against both human and vehicle penetration, while detracting less from the aesthetics of a facility than their manmade counterparts. Natural barriers include hills, outcroppings, lakes, ponds, hedgerows, rocks, and timber. They can be naturally occurring, or can be manmade by relocating natural materials. Some of the most common natural barriers are vegetation, water, and terrain[14]:

[14] http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/DesignConsiderations/CD/appd.htm

- Vegetation: Vegetation along standoff zone perimeters and on off-road approaches to the perimeters can deter aggressors from approaching the protected facility from that route. Vegetation may also slow the approach of vehicles by providing obstacles to direct approach. Closely spaced plants in multiple, overlapping rows with trunk diameters greater than five inches are the best deterrents to stationary vehicles. Perimeter barriers capable of stopping moving vehicles can be integrated with plantings of vegetation for aesthetics purposes. Because mature plants are the most effective deterrents, the plant material should be provided by retaining existing vegetation where possible.

- Water: The effectiveness of bodies of water used as barriers to moving vehicles has not been quantified, but their value in slowing vehicles and as a deterrent is obvious. Water that is deep enough to submerge the exhaust pipes of vehicles will provide an effective barrier. Lesser depths may only slow vehicles. For example, cars and light trucks will be limited to speeds of approximately 25 miles per hour by large bodies of water only 6 inches deep. Bodies of water three feet deep would act as barriers to moving vehicles. If the body of water floor is uneven or contains several deep trenches, the effectiveness as a barrier increases significantly.

- Terrain: Terrain features such as ditches, berms, hills, or large rocks may provide effective barriers to vehicles. Rocks or groups of rocks that have a collective mass equal to approximately twice that of the threatening vehicle make effective barriers. To be effective, rock ditches, and berms must span the approach route to block it. Those of lesser extent or such features of a size too small to stop a vehicle can be used as obstacles to slow vehicle approaches. In designing terrain obstacles, circuitous, off-road approach routes are far more effective than direct routes. As an example, the use of inclines can slow vehicle approaches by limiting their ability to accelerate.

Security Considerations for Perimeter Barriers

The choice of an appropriate barrier is not only affected by the cost of the equipment, installation, and maintenance, but also by the more important aspects of effectiveness and functionality. Certainly the highest consideration in an effective boundary measure is its ability to prevent unauthorized penetration. Unfortunately, no one barrier-type provides the security solution to all types of adversaries.

The facility perimeter may be of a number of different designs at various locations due to a variety of natural and operational reasons. A "layered" approach to perimeter barriers and monitoring potentially increases the opportunity to reduce cost and uses existing facility natural features or more applicable technologies to meet the performance objectives.

An owner/operator may wish to consider the benefits and costs related to completely enclosing a large facility footprint within a single perimeter versus implementing multiple smaller restricted area perimeters.

The owner / operator may achieve a higher level of security performance by deploying barriers behind the intrusion detection system so that an intruder would activate an alarm sensor before defeating the barrier(s), thereby providing additional delay for assessment and response. Barriers located in front of alarm sensors serve to mark property boundaries and may keep people and

animals from wandering onto a facility, but they provide little or no additional response time because an adversary can usually breach the barrier without activating any intrusion detection sensors.

Access points work best when they permit passage of authorized persons with relative ease. While the number of access points should be kept to a minimum, access points typically are needed for routine, maintenance, and emergency operations.[15]

Performance Standards Affected by Perimeter Barriers

The implementation of perimeter barriers can have a significant impact in helping a facility achieve RBPS 1, 2, 3, and 4. Perimeter barriers can also have a smaller or secondary impact on meeting RBPS 6 and 13.

Additional Resources on Perimeter Barriers

PERIMETER BARRIERS	
RESOURCES	**SOURCES**
Protection of Assets Manual, ASIS International	http://www.protectionofassets.com/ (Access available through: www.asisonline.org)
Chain-Link Fabric Security Fences and Gates, Australian Standard AS 1725-2003, prepared by Chainwire Security Fencing Committee.	Available through: www.ansi.org
"*Chain Link Fence Manufacturer's Institute Security Fencing Recommendations,*" Chain Link Fence Manufacturers Institute	http://codewriters.com/asites/page.cfm?usr=clfma&pageid=887
Department of Army Field Manual 3-19.30, Physical Security, Chapter 3, *Design Approach,* January 8, 2001	www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch3.htm
Department of Army Field Manual 3-19.30 Physical Security, Chapter 4, *Protective Barriers,* January 8, 2001	www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch4.htm
"*Security and Force Protection,*" DRMS-1-4160.14 Vol. 1, Chapter 2, Defense Reutilization and Marketing Service, Defense Logistics Agency	www.drms.dla.mil/publications/4160.14/section1/s1c4.pdf
Electrical Installations – Electric Security Fences, Australian/New Zealand Standard AS/NZS 3016:2002	Available through: www.ansi.org
From Jericho to Jersey Barrier By Richard Kessinger, CPP	www.sloanfencing.com/Documents%20and%20Settings/63/Site%20Documents/Crash%20Rated%20Solutions%20From%20Jericho%20to%20Jersey%20Barrier.pdf
Glass in building. Security glazing. Testing and classification of resistance against bullet attack. BS EN 1063:2000	Available through: www.ansi.org
Introduction to Security, Sixth Edition, Robert J. Fischer, Gion Green, Butterworth-Heinemann, 1998 (ISBN: 0-7506-9860-8)	Available through numerous booksellers online
Navy's Physical Security Equipment Program and Anti-terrorism Services, Antiterrorism and Force Protection Ashore Program (ATFP Ashore)	http://atfp.nfesc.navy.mil/atfp_faq.html

[15] DHS, Transportation Security Administration, *Recommended Security Guidelines for Airport Planning, Design and Construction*, June 15, 2006

Crime Prevention Through Environmental Design	www.cpted.net
Transit Security Design Considerations, Federal Transit Administration (FTA) Office of Research and Innovation, U.S. Department of Transportation	http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/DesignConsiderations/CD/front.htm#toc

Monitoring

Security events are monitored through a combination of human oversight and a variety of technical sensors interfaced with electronic entry-control devices, remote surveillance imagery, and alarm reporting displays. When an event of interest to security is identified, it is either assessed directly by sending persons to that location or remotely assessed by personnel evaluating sensor inputs and surveillance imagery.

Types of Monitoring

An integrated technical security system frequently includes sensors; CCTV or thermal imaging cameras for assessing alarms; electronic access control; means of transmitting the data; and a reporting system for monitoring, controlling, and displaying information on security events. The owner / operator may wish to consider each of several interrelated elements of the perimeter security system:

- Intrusion Detection System, Alarm Display, Video Assessment, and System Integration

The owner / operator may consider various display and annotation systems to enhance the efficiency and effectiveness of monitoring the perimeter security system, including:

- Programming a video system controller to perform video functions automatically and start recording the alarm scene and entering time / location data.
- Sets of video monitors can display identical information at different locations or different times, providing live and recorded scenes for evaluation.
- Connecting the video controller to a host computer that collects and processes alarm information, to store alarm scenes within milliseconds after the alarm occurs, bypassing and enhancing manual control.
- Attaching the video switcher to a host alarm computer can enhance archiving by recording real-time and alarm playback scenes.
- Alarm data back-up to avoid loss in the event of main computer failure or line cuts between the multiplexers.

Intrusion detection systems provide early warning of unauthorized penetration, and each system consists of various hardware and software elements operated by trained personnel with security responsibilities. The owner/operator may wish to consider locating these functions in a command and control center. Consideration for command and control centers may include merging security monitoring and reporting systems with other systems such as fire engineering reporting systems or process control. Technical merger of an active security system and a passive fire system may facilitate a common set of operational procedures (e.g., reporting, training, and emergency response). Intrusion detection, which monitors for attacks, is less a preventative measure and more of a response measure; although some would argue that it is a deterrent. Intrusion detection has a

high incidence of false alarms. In many jurisdictions, law enforcement will not respond to alarms from intrusion detection systems.

The goal of command and control center is to synchronize the different elements of access control and screening technologies into a centralized location.

Intrusion Detection System

Intrusion detection systems (IDS) provide early warning of unauthorized penetration. IDS typically consist of various hardware and software elements operated by trained personnel with security responsibilities. The system triggers an alarm or other notice of an attempted breach, which can be used for activating corresponding cameras or for dispatching personnel to investigate the alarm.

There are limitless possible configurations of intrusion detection system (IDS) components that together satisfy the RBPS for securing and monitoring the facility perimeter. The expectation is for each owner / operator to implement and configure a set of security countermeasure components for their respective facility that will meet or exceed the expectations of the RBPS for the facility Tier metric applicable to their facility.

As reflected in the table below, a wide variety of technical security elements for consideration by the owner / operator can comprise systems that meet the RBPS. These elements generally fall into five major categories:

- Fence-mounted sensors
- Beam sensors
- Open-area sensors
- Remote surveillance
- Human-based elements

Table A2: Common Technical Security and Intrusion Detection System Elements

Fence-mounted Sensors	Beam Sensors	Open Area Sensors	Remote Surveillance	Human-based
• "Break Wire" sensor • Balanced pressure-line • Buried geophone • Capacitance sensor • E-field sensor • Fiber-optic cables • Intelligent	• Infrared (IR) break beam • Passive infrared sensors	• Acoustic sensor • Active infrared • Buried line sensors • Intelligent video • Magnetic-field sensor • Microwave or volumetric sensors • Mono-static or	• CCTV cameras • Thermal imagers • IP Cameras	• Protective forces, dedicated (posted) • Protective force - roving patrols • Dedicated operators • Local law enforcement

Table A2: Common Technical Security and Intrusion Detection System Elements				
Fence-mounted Sensors	**Beam Sensors**	**Open Area Sensors**	**Remote Surveillance**	**Human-based**
video • Magnetic polymer • Ported coaxial cable • Taut wire sensor • Vibration-detection sensors • Video motion detection		bi-static sensors • Passive infrared • Photoelectric motion detector • Radar • Vibration detection sensor • Video motion detection		

The desired intrusion detection system provides a high probability of detecting and reporting intruders into the restricted area perimeter, and accomplished through a variety of perimeter and critical area protection measures. General principles for consideration include:

- A continuous line of intrusion sensors around the areas to be protected.
- Multiple lines of detection used to achieve protection-in-depth at critical assets.
- Complementary sensors covering the same area, but using different means of detection (such as a video camera used in conjunction with an alarm), decrease the probability of defeat.
- Alarm combination and priority schemes enhance system effectiveness.
- Tamper protection on junction boxes and sensor housings minimizes bypass attacks.
- Sensors placed in clear zones (i.e., zones that are not subject to environmental disturbances, such as foliage, birds, squirrels, etc.) are more easily assessed and are less prone to nuisance alarms.
- Exterior sensor systems in combination with other perimeter security systems may reduce protective force staff size and the reliance on staffed checkpoints.
- Nuisance alarm rates due to environmental causes (wind, rain, birds, etc.) should be a major consideration for technical applications.

Control systems can be vulnerable to a variety of attacks. Securing control systems poses significant challenges, including limited specialized security technologies and lack of economic justification.[16]

[16] Government Accountability Office, *Crticial Infrastructure and Protection: Challenges and Efforts to Secure Control Systems*, March 2004 (GAO-04-354)

CCTV

CCTV surveillance systems have proven their worth for facility security over a period of more than 40 years. The equipment is relatively inexpensive compared to other means of surveillance, provides detailed images of scenes for positive assessment of what is happening, operates for years with minimal maintenance, and requires minimal operator training.[17]

When CCTV cameras are used, these additional lighting considerations should be taken[18]:

- Color Rendering Index: Choose an appropriate lamp that has accurate color reproduction.
- Reflectance of Materials: Consider material that will be illuminated, and its ability to reflect and transmit light.
- Direction of Reflected Lighting: Identify whether reflected lighting will assist or interfere with camera operation.

Intelligent Video[19]

Intelligent video originated with motion detection circuits which detected changes in the characteristic of the video signal in a defined area of the screen, known as a window. An operator could then be alerted to an event as it happened, greatly reducing the need for operators to stare at video monitors for long periods of time. The effectiveness of this technology has improved, especially in digital systems where software has been developed to cope with shadowing, blowing trees, and other environmental effects which created false positive alerts in early systems.

Digital video systems are now able to detect multiple objects in a scene (and exclude areas of the scene) and track objects as they move across the scene.

Security Considerations for Monitoring

Perimeter monitoring system is less a preventative measure and more of a response measure. Intrusion detection has a high incidence of false alarms.

When electronic components are included in the perimeter monitoring system, the owner/operator may wish to locate alarm reporting devices and video monitors in a command and control center. To increase the reliability of a monitoring system, an owner/operator may elect to deploy multiple interactive, redundant, or sophisticated sensors or counter-measures at high-risk locations with the understanding that increased reliability also extends to the functional capabilities of the data-transmission system.

Performance Standards Affected by Monitoring

---

[17] DHS, Transportation Security Administration, Recommended Security Guidelines for Airport Planning, Design and Construction, June 15, 2006

[18] ASIS 2004, Chapter 19 – Security and Protective Lighting

[19] DHS, Transportation Security Administration, Recommended Security Guidelines for Airport Planning, Design and Construction, June 15, 2006

The implementation of monitoring systems can have a significant impact in helping a facility achieve RBPS 1, 2, 3, and 4, and 10.

Additional Resources on Monitoring

MONITORING	
IDS Sensors, Perimeter Sensors, Line Sensors, IDS Maintenance	
RESOURCES	**SOURCES**
CCTV for Security Professionals, Matchett, Alan, Butterworth-Heinemann, 2003 (ISBN: 0-7506-7303-6)	Available through numerous booksellers online
"*Assessing the impact of CCTV*," Gill, Martin and Spriggs, Angela, UK Home Office Research Study 292, Home Office Research, Development and Statistics Directorate February 2005	www.asisonline.org/newsroom/crisisResponse/cctv.pdf
Department of Army Field Manual FM-3-19.30 Physical Security, "*Electronic Security Systems*," Chapter 6, January 8, 2001	www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch6.htm
Effective Physical Security, Part Two/ Equipment, Chapter 9. Alarms: Intrusion Detection Systems, Third Edition, Fennelly, Lawrence J., Butterworth-Heinemann, 1997 (ISBN: 0-7506-9873-X)	Available through numerous booksellers online
"*Walk-Thru Metal Detectors for Use in Concealed Weapon and Contraband Detection*," Law Enforcement and Correction Standard and Testing Program, National Institute of Justice, NIJ Standard 0601.02, Department of Justice, January 2003	www.ncjrs.gov/pdffiles1/nij/193510.pdf
Perimeter Security Sensor Technologies Handbook, Defense Advanced Research Projects Agency (DARPA), 1997	www.nlectc.org/perimetr/full2.htm
The Design and Evaluation of Physical Protection Systems, Part Two, Design Physical Protection Systems, Garcia, Mary Lynn, Butterworth-Heinemann, 2001 (ISBN: 0-7506-7367-2)	Available through numerous booksellers online
Unified Facilities Criteria: UFC 4-022-01, *Security Engineering: Entry Control Facilities / Access Control Points* (05-25-2005), Department of Defense	www.wbdg.org/

Security Lighting

Security lighting can help to both deter attempts at penetrating a facility's perimeter and assist in the monitoring and detection of any such attempts. Inadequate lighting can make it more difficult to monitor a perimeter and detect attempts to breach the perimeter either directly through human protective forces, or through certain types of monitoring and intrusion detection systems, such as

CCTVs. Due to the increased likelihood of detection based on appropriate security lighting, maintaining a well lit facility perimeter also can help deter adversaries from attempting to breach that perimeter. A wide variety of different types of security lighting is available for implementation at facilities.

Security Considerations for Security Lighting

When determining if security lighting is an appropriate part of a facility's security posture and what type of lighting to choose, a facility should consider such items as available power sources, grounding, and interoperability with and support to other monitoring and detection systems, such as CCTVs. Local weather conditions/environmental conditions can also significantly affect sensor and lighting performance. For example, certain sensors or other IDS components that have near perfect detection capabilities during good weather might be subject to unacceptably high levels of false alarms during inclement weather (e.g., fog, rain, wind). Similarly, security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather. Accordingly, an owner/operator should consider the impact of environmental conditions when making determinations regarding security lighting.

Performance Standards Affected by Security Lighting

The implementation of security lighting can have a significant impact in helping a facility achieve RBPS 1, 2, 3, and 4, and a smaller impact on RBPS 6, 7, and 9.

Additional Resources on Security Lighting

LIGHTING SYSTEMS	
RESOURCES	**SOURCES**
Effective Physical Security, Part Two, Chapter 8, Security Lighting, Third Edition, Fennelly, Lawrence J., Butterworth-Heinemann, 1997 (ISBN: 0-7506-9873-X)	Available through numerous booksellers online
Exterior Security Lighting, Section 4.7 of Mil-HDBK-1013/1A, Design Guidelines for Physical Security of Facilities, 1993	assist.daps.dla.mil/quicksearch/basic_profile.cfm?ident_number=54120
Guideline on Security Lighting for People, Property, and Public Spaces, GL-1-03, The Illuminating Engineering Society of North America	www.iesna.org/shop/item-detail.cfm?ID=G-1-03&storeid=1
Introduction to Security, Chapter 8. The Outer Defenses: Building & Perimeter Protection, Lighting, Seventh Edition, Robert J. Fischer & Gion Green, 1998 (ISBN: 0-7506-9860-8)	Available through numerous booksellers online
Lighting Research Center Webpage	www.lrc.rpi.edu/researchTopics/applicationsDesign/securityResources.asp
Department of Army Field Manual 3-19.30, Physical Security, Chapter 5, *Physical Security Lighting*, January 8, 2001	www.globalsecurity.org/military/library/policy/army/fm/3-19-30/ch5.htm#pgfId-1024523

Security Forces

Protective forces are often used to enhance perimeter security and provide a means of deterrence, detection, delay, and response. Such forces can be proprietary or contracted, and can be armed or unarmed. Protective forces can be used in a variety of ways, including standing post at critical assets, monitoring critical assets using remote surveillance, or conducting roving patrols on a documented schedule that specifically includes identified targets, processes, or assets. Protective forces may be qualified to interdict adversaries themselves, or simply to deter and detect suspicious activities and to then call local law enforcement to provide an interdiction.

Security Considerations for Security Forces

No matter how they are deployed, protective forces alone generally do not provide sufficient perimeter security. Accordingly, if a facility employs protective forces, they likely will need to be used in combination with one or more of the other measures listed above to provide an appropriate level of security to meet the Restrict Area Perimeter performance standard.

Performance Standards Affected by Security Forces

The use of security forces can have a significant impact on every single RBPS.

Additional Resources on Security Forces

PHYSICAL SECURITY	
RESOURCES	**SOURCES**
Protection of Assets Manual, ASIS International	http://www.protectionofassets.com/ (Access available through: www.asisonline.org)
Installation Antiterrorism Force-Protection Planning	http://usacac.leavenworth.army.mil/CAC/milreview/download/English/MarApr02/flynn.pdf
Terrorism Knowledge Base, National Memorial Institute for the Prevention of Terrorism website	www.tkb.org/Home.jsp
DoD Minimum Antiterrorism Standoff Distances for Buildings, UFC 4-010-10	http://www.acq.osd.mil/ie/irm/irm_library/UFC4_010_01-31JUL2002.pdf
Part One: Design, *Effective Physical Security*, Second Edition, Lawrence J. Fennelly	Available through numerous booksellers online
Force Protection 2001, National Defense University	www.jfsc.ndu.edu/library/publications/bibliography/force_protection.asp
Introduction to Security, Part III – Basics of Defense, Seventh Edition, Robert J. Fischer, Gion Green, Butterworth-Heinemann, 1998 (ISBN: 0-7506-9860-8)	Available through numerous booksellers online
Risk Analysis and The Security Survey, James F. Broder, CPR, Second Edition	Available through numerous booksellers online
Risk Management for Security Professionals, Carl A. Roper (ISBN 0-7506-7113-0)	Available through numerous booksellers online
Securing the ports of NY & NJ, Submitted by Steven's Institute of Technology	www.stevens.edu/main/home
The Design and Evaluation of Physical Protection Systems, Mary Lynn Garcia, Sandia National Laboratories	Available through numerous booksellers online
Unified Facilities Criteria, DoD Minimum Antiterrorism Standards for	www.tisp.org/files/pdf/dodstandards.pdf

Buildings, UFC 4-010-01, July 31, 2002	
American Chemistry Council Guidance on Conducting Contractor Background Checks	www.responsiblecaretoolkit.com/pdfs/Background.pdf
Guide to Background Checks, Illinois Association of Chiefs of Police	www.integrasecurity.org/GuideMay2004.pdf
Introduction to Security, Seventh Edition, Chapter 8, The Outer Defense, Building and Perimeter Protection, Robert J. Fischer & Gion Green	Available through numerous booksellers online
Mil-HDBK-1013/1A, December 15, 1993, *Design Guidelines for Physical Security of Facilities*	http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf
Specific Countermeasures at USCG webpage	http://homeport.uscg.mil/mycg/portal/ep/channelView.do?channelId=-18389&channelPage=/ep/channel/default.jsp&pageTypeId=13489
Vehicle Inspection Checklist and other related documents are available on the Technical *Support Working Group* website	www.tswg.gov
Handbook of Information Security Management, The CISSP Open Study Guides Web Site	www.cccure.org/Documents/HISM/ewtoc.html
United Facilities Criteria (UFC) Security Engineering: Entry Control Facilities/Access Control Points, Department of Defense, May 2005, UFC-4022-1	www.wbdg.org/ccb/DOD/UFC/4_022_01.pdf
Government Emergency Telecommunications Service, National Communications System (NCS) 2004	http://gets.ncs.gov/

Cyber Security Measures

A wide variety of policies, procedures, and measures are available for helping secure a facility's cyber system from attack or manipulation. They include the following: (1) security policy, (2) access control, (3) personnel security, (4) awareness and training, (5) monitoring and incident response, (6) disaster recovery and business continuity, (7) system development and acquisition, (8) configuration management, and (9) audits.

Types of Cyber Security Measures

Security Policy

Security policies, plans, and procedures. A typical starting point for any cyber security program is documented policies, plans, and procedures, all of which are related but serve distinctly different purposes:

- A *policy* is the highest level document that states what a company, group, or department will and will not do. An example of a policy is a document that states, "All data will be secure," "Change management processes will be followed for all projects," "Systems with a high availability rating will be online 99.999% of the time" or "IT security will be effectively managed on all systems including access control and business systems."
- A *plan/process* is the document that describes a methodology for how to achieve the policy's goals. An example of a plan document might be a System Security Plan that makes statements such as, "All public facing web servers use Secure Sockets Layer (SSL) certificates with mandatory 128bit encryption," or "all systems perform nightly incremental backups and weekly full backups."
- A *procedure* is the step-by-step instructions to the employee for exactly how something is to be done. A procedure document will detail steps and contain statements such as, "Step One: order SSL certificate from Vendor X. Step Two: Install certificate on web server. Step Three: Test using multiple web browsers." A procedure will often go into even greater detail by stating exactly which options to choose and what buttons and options to physically click on to accomplish the goal.

Security policies, plans, and procedures that specifically address operational constraints, sensitivity issues, and processing environment issues can be addressed in general information technology (IT) documentation or specified in their own dedicated documentation.

Formal change management process. A change management process is a process outlining the steps an organization will take to request, evaluate, plan, implement, and measure the impact of a change to a system. Good cyber security calls for a formal change management process that is both documented and distributed to relevant parties. Without a defined process that takes into account policy mandates, security concerns, business impact, authorization, and oversight, changes can weaken the stability and security of a system. A cyber change management process ensures the most effective and efficient application of network and system updates, reduces the likelihood of the introduction of malicious code, and reduces the chance of human error.

Generally, monitoring of changes is done through a formal cyber change management process which should have documents outlining the entire change process, including testing prior to introduction of new or changed components into the operational environment. In addition to procedural documents, audit logs often are kept documenting who made changes to what and when.

Formal designation of a cyber security officer. Formally designating an individual to be responsible for cyber security helps establish management support for cyber security as well as providing direction, accountability, and oversight to cyber security. Examples of qualified cyber security individuals include:

- Chief Information Officer
- Information Technology Cyber Security Specialist
- System Administrator
- Certified Information Systems Security Professional

Access Control

Verifying and managing external connections. Understanding and managing connectivity—i.e., the possibility of transferring data electronically (e.g., through external access such as the wireless connection or portable cyber equipment such as flash drives)—is an essential component of cyber security. Because cyber vulnerabilities can be exploited in many ways, connectivity is not as simple as whether or not a wired connection to the Internet is openly in use. Network back doors exist in the form of wireless connections, modems, portable electronic devices and media such as laptop computers, personal digital assistants (PDA), universal serial bus (USB) drives, compact disks (CD), or floppy disks, etc. Only by verifying external connections through the use of network tools designed for this purpose can managers be certain of the security environment of their systems and networks.

It is also good cyber security practice for all external connections to/from critical systems to have a documented business need and for organizations to have a policy that no new connections can be established without management authorization and documentation. Examples of external connections to a system or network are modems used to dial in for maintenance or to access data; connections between control systems and business systems; or Internet accessible nodes like firewalls, routers, mail servers, web servers, and Domain Name System (DNS) servers.

A common misconception regarding connectivity is if an organization does not subscribe to an Internet Service Provider, it is not connected (often referred to as "air gapped"). Often ignored are wireless devices not visibly plugged in (e.g., wireless Local Area Network (LAN), wireless sensors, and wireless cameras); and modems that may or may not be enabled all the time, and may or may not be under control of the organization (e.g., vendor provided). Testing (i.e., scanning) is the only effective way of detecting these unseen connections. Employee actions including the use of portable devices and/or media can be as effective a means of connecting to internal assets, systems, and networks as an Internet connection.

The "least privilege" concept. The concept of "least privilege" means people are only granted as much access as they need to perform their assigned job function, and no more. Examples of the

least privilege concept in action include allowing only appropriate personnel being to access business proprietary data or allowing only systems administration personnel access to system-level files and permission to grant access rights to other users.

Password Management. Managing passwords is a key component of a good cyber security program. Successful password management includes immediately changing all default passwords provided with any systems or applications, and establishing appropriate parameters and rules that for password structure.

Default Passwords. Most systems and applications are installed with a factory default password that needs to be changed. If default passwords are not immediately changed, unauthorized individuals familiar with a product may be able to access it. This is especially true considering that default passwords are often posted on Internet web sites. Typical systems and applications with default passwords include firewalls, programmable switches, major application installations, and routers. Some applications, such as database software, often contain multiple default passwords. Administrators unfamiliar with the product may only change one password without realizing additional passwords need to be reset. Accordingly, good cyber security practice includes ensuring that all default passwords are changed for every system and application a facility possesses.

Password Structure. There are many parameters and rules that can be applied to a password structure. Typical rules focus on the structure of the password (e.g., passwords must be at least 7 letters and require at least one uppercase and one lower case letter), and the frequency of password changes (e.g., requiring a user to change his or her password every 90 days). It is important to find an appropriate balance between complexity and frequency of change, and the associated business needs and practicality. Larger passwords requiring special characters are more secure, but harder for users to remember. Regardless of what password structure is chosen, the system should be structured so that all passwords meet the mandated attributes before they are accepted. Likewise, if a facility requires its employees to change their passwords every 90 days, to be effective, the system should track timeframes, remind users when it is time to change their password, and then enforce the change.

Proper configurations to limit access. Business and control networks often are connected for efficiency or economy, or because common or public networks are used for communications or as integral parts of the larger system. Unfortunately, this opens the control systems network to the vulnerabilities of the general business infrastructure, including the Internet—issues for which they were not designed, and often are not managed. Firewalls can be used to control access, but most firewalls common in the industry today do not inspect for valid control system protocol contents, thus making the firewall an ineffective barrier between the systems. Firewalls utilized in control system environments should support, understand, and filter control system specific protocols (e.g., Intercontrol Center Communications Protocol (ICCP)). Other methods exist for configuring the networks to limit access to control systems, e.g., segregating business and control networks, but this may impact efficiency or economy and should be considered as part of a joint business/security decision.

Rules governing interconnections. Many systems are interconnected. A good cyber security posture typically includes rules governing interconnections, especially when these connections are to components outside of the organization's direct control. This includes ensuring that remote connections to all control systems, components, and devices are addressed, to include remote terminal unite (RTU)'s, programmable logic controllers (PLC)'s and end unit devices (actuators,

sensors, valves, etc.). Remember, if Company A has an open connection to Company B, Company A is only as secure as Company B.

Personnel Security

Role-based access rights. It is a good cyber security practice to review all roles to determine what types/levels of sensitive materials someone filling that role is allowed access to. Assigning a "high," medium," or "low" rating to a role is a standard labeling process, and can be very useful so long as those terms are well defined for the business. An example rating would be a rating of high for system administrators.

Additionally, although people often fill multiple roles within an organization, each role and its related security needs should be defined and separated. This allows for natural checks-and-balances, which is key for preventing human error and internal misuse of systems and information.

Two roles that a facility should strongly consider separating are the IT Security and Systems Administrator, as they often have natural conflicting goals (more secure vs. faster or more efficient). When both roles are assigned to the same individual, organizations are left with the potential for a conflict of interest. For the highest risk facilities, it is often good to have separate individuals in charge of IT Management, IT Security, and System Administration. For lesser risk facilities, simply separating the System Administrator and the individual in charge of IT security should suffice.

Providing individual user accounts. When accounts are shared among multiple individuals, it cannot be determined which user is responsible for a given action. Additionally, if a security breech occurs it can be difficult to identify the source of that breech if it comes from a shared account. Accordingly, providing individual user accounts where technically feasible is good cyber security.

The most common violation of this basic security rule is found with the administrator account on a given system, particularly with the root account on UNIX systems. Although each user and/or administrator may have their own account, it is often more convenient to log in using the default administrator account to perform maintenance and other activities. When this account is shared and a problem with the system or with missing data arises, it can be impossible to identify who is accountable. Another example of this practice occurs in control systems environments that operate on a 24/7 schedule. A user may log in at the beginning of their shift and leave their account logged in after they have left and the next shift has taken over or a group account may be used.

In some control systems environments it may be standard practice to use a single group account for multiple users. Management may make a risk based decision to allow this practice for business purposes; however, the risk associated with that decision should be managed with other security controls.

Managing changes in roles. Actively managing access for changing roles of employees (e.g., termination, transfer, demotion) ensures that only appropriate access is allowed. Immediate review of all role changes is recommended. For all employees who have departed under adverse circumstances, however, it is recommended that all access rights (both physical and electronic) be revoked by close of business the same day. This includes immediate revocation of system and

application accounts, e-mail access, keys, keycards, and all other credentials immediately upon termination of an employee without exception.

Managing external service providers. External service providers, business partners, and vendors could potentially present risk to an organization's cyber security. Ensuring that partner organizations subject their personnel to security requirements acceptable to you if they are to have access to your facilities, systems, information, and intellectual property is good cyber security. Common tools to manage this include memoranda of agreements, non-disclosure agreements, confidentiality agreements, and conflict of interest agreements.

Awareness and Training

The human component is often the most vulnerable aspect of a system. As a result, a good cyber security program generally involves making system users aware of the need for security and instructing them on their role in keeping the cyber system secure. A documented cyber security training program, which establishes types and frequency of training, is the best way to accomplish this. Cyber security training can include group briefings, online instruction, or written policy and procedure reviews, and basic topics that a facility may want employees to be trained on include:

- General company policy review
- Roles and responsibilities
- Password procedures
- Acceptable practices
- Whom to contact and how to report suspected inappropriate or suspicious activity.

Training is most effective when refreshed and reinforced on a predetermined schedule, and training courses are updated to reflect the changing threat and vulnerability environment. An effective training program may provide for different training regimens are appropriate for employees with different roles. For example, system administrators typically need more training than standard users because of their access to highly sensitive material. Also, training for personnel requiring access to proprietary information is not necessarily warranted for all employees.

Monitoring and Incident Response

Computer Emergency Response Function. Incident response is an important part of a comprehensive cyber security program, and a good cyber security program typically will include a defined Computer Emergency Response function that can be contacted in the event of a cyber emergency and that is specially trained to identify, contain, and resolve a cyber intrusion, denial of service attack, virus, worm attack, or other cyber incident.

Network Monitoring. Facilities monitor networks for unauthorized or malicious access to maintain situational awareness and mitigate risk. An intrusion detection system (IDS) can be used to monitor networks. An IDS is a system designed to capture network or host traffic, analyze it for known attack patterns, and take specified action when it recognizes an intrusion or attempted intrusion. An IDS can be software or hardware, and can be network-based (i.e., captures and analyzes all network traffic) or host-based (i.e., installed on, and analyzing traffic for, a single device). Hardware solutions are more suitable for larger volumes of data. There are several open source IDS applications available for free download. For best results, IDS utilized in control system

environments should understand control system traffic and protocols and should detect unusual or unexpected control systems traffic.

Event recognition and logging. Recognizing and logging events and incidents is critical to overall system and network security. Recognizing security events for what they are and making management aware of the incidents and their potential for harm is a critical element in obtaining the appropriate support and resources to effectively manage cyber security, thus limiting the damage from future cyber attacks. Logging incidents and frequently reviewing the log files helps ensure that threats to system security are addressed promptly, stability is maintained, and systems are operating at maximum efficiency. Administrators use log files to understand typical system behavior and how it will vary preceding and during an incident. Good cyber security includes scheduled log reviews and maintenance of evidence that they were reviewed. An automated review of log files is most desirable as it is done continuously while a manual review is a laborious process.

Watchdog Systems. Watch-dog systems are systems that take action when something goes wrong on the cyber system, typically providing interlocks or responses to prevent or mitigate catastrophic events and/or consequences of a cyber attack. A safety watch-dog system is an independent system implemented for the purpose of taking a process to a safe state when pre-determined conditions are violated. Examples of watchdog systems include Safety Instrumented Systems (SIS) and Plant/Reactor Protection Systems.

Recently, the trend has been toward networking these systems with the control systems they stand to protect. By doing this, the watch-dog systems are subject to the exploitation of the same vulnerabilities. In order to assure that watchdog systems are available and functioning as expected, these systems should be separately secured. One way to do this is through a firewall which recognizes control and watch-dog system protocols, thus effectively separating both systems.

Many events are low-order and do not rise to the level of reporting to management. These are typically events that are handled appropriately by firewalls. Those that get by or that do damage need to be reported to management. The more severe the damage, the higher the reporting should be.

Malicious Code Prevention. Viruses, worms, Trojans, and other malicious software code proliferate on the Internet and mutate on an unpredictable basis. Malicious code is so common that without automated protection it is a near certainty that systems will be infected. Even without access to the Internet, malicious code can be introduced to an organization through actions (even unintended) of employees, support personnel, vendors, and business partners. Antivirus software can be implemented on a facility's system when architecture and application permit it, and such software should be updated on a regular basis, preferably automatically. Scheduling DAT updates is best done in the software itself, configured at the time of installation; manual tracking of recent developments and application of protective measures generally is insufficient.

For control systems where system architectures or operational requirements may not permit the use of antivirus software, layered defenses can be used to prevent the events or intrusions from reaching vulnerable control systems.

With the prevalence of e-mail borne viruses and other spam messages including malicious software attachments, it is best practice for owner/operators to filter e-mail attachments (e.g., executable

files) for control systems that have e-mail, and apply some level of filtering that will remove attachments with dangerous file extensions. Filtering of email attachments can be done at either the individual workstation or more effectively at the e-mail server which routes all messages to recipients. Examples of files known to have the ability to propagate worms and viruses are ".exe," ".zip," and ".jpg."

Disaster Recovery and Business Continuity

A good cyber security posture typically also include Continuity of Operations Plans (COOP), IT Contingency, and Disaster Recovery Plans for its critical cyber assets, all of which incorporate cyber security considerations during contingency operations and recovery/reconstitution activities. As recovery operations (i.e., those operations addressed in COOP, IT Contingency, and Disaster Recovery Plans) are often done under pressure, systems often are vulnerable when they are underway, and thus it is important to consider cyber security during such operations. Examples would include ensuring that cyber security best practices are followed when setting up an alternate system or network and when rebuilding and reconfiguring the primary systems and networks.

System Development and Acquisition

Integrate cyber security into development lifecycle. Including cyber security throughout the development lifecycle, from system design through procurement, implementation, operation, and disposal, is good cyber security. By integrating system security into the existing development lifecycle, a facility can ensure that money is budgeted, personnel are designated, and requirements are gathered for security at appropriate times rather than after it is inconvenient, prohibitively expensive, or impossible.

One example of incorporating cyber security into the development lifecycle is having statements and steps to follow regarding cyber security in developmental plan documents. For instance, during a requirements gathering phase, cyber security may be a foundation issue; all system design changes consider the impact on cyber security before being approved and during implementation; and critical or sensitive information is cleansed from systems prior to disposal or redeployment.

Configuration Management

Maintain inventory of cyber infrastructure: Maintaining a current inventory of the components of a cyber infrastructure has numerous benefits, including supporting the locating, tracking, diagnosing, and effective maintenance of cyber assets.

Examples of items to be inventoried include internet access points, web sites, Virtual Private Networks (VPN), gateways, routers, firewalls, wireless access points, modems, vendor maintenance connections, Internet Protocol (IP) address ranges, Remote Terminal Units (RTU), Programmable Logic Controls (PLC), access control systems, closed circuit television (CCTV) systems, private branch exchange (PBX) telephone systems, alarm systems, fire control systems, radios, wireless devices, servers, proxies, workstations, and printers. For control systems, inventory of internal network nodes may also want to include IP enabled field controllers and field devices.

It is a good idea to inventory all external communications media and components, including modems, network configurations (e.g., Ethernet, token ring, ATM, Sonet), dial-up modem lines,

point-to-point leased lines, wireless (e.g., 802.11 standard wireless local area network, Bluetooth, satellite, microwave), and VOIP, as each component must be known in order to be secured. Because external communications media and components can be used not only for remote connections, but also by vendors for remote maintenance, they have the potential for allowing individuals unknown to system operators or beyond their control (even sometimes outside of the range of phone lines in use by the company, thus masking them from normal efforts to detect and manage) to have access. If not identified and properly managed, these components can leave systems open to vulnerabilities.

Documenting business needs. It is good cyber security practice for all applications and services (e.g., operating systems, databases, e-mail, office applications, Internet browsing, Voice Over Internet Protocol (VOIP)) to have a documented business need and for organizations to ensure that no new applications or services can be installed or enabled without management authorization and documentation where technically feasible.

Regular patches and updates. As new vulnerabilities are discovered in operating systems and software applications, patches and other updates are released to deal with them. Updating systems and networks with these patches should be done on a scheduled basis and should follow a documented procedure. The complex nature of systems and networks occasionally introduces secondary vulnerabilities in an attempt to remedy another. Regular updates ensure that these also are countered in a timely and effective manner. The most common example of this is the regular releases of security patches for operating systems by software vendors.

Audits

Audits are generally considered essential to maximize the effectiveness of the cyber security measures that have been put in place. Facilities with strong cyber programs typically will report the results of audits to senior management so that findings can be understood and agreed upon, and mitigated with management support. If planned properly, audit requirements and assessments can be established that minimize the risk of disruption to business processes. A regular program of IT audits typically will involve the development of a schedule; checklists for use during the audits; procedures for carrying out audits; and recording, analyzing, and reporting findings.

Security Considerations for Cyber Security Measures

Potential Off-site Aspect of Cyber Security

Given the nature of today's information technology environment, it is not unusual for IT equipment, IT data, or even IT staff to be located off-site. For instance, corporations with multiple facilities may keep central data servers and processing units in a single location at one facility, may only have cyber security officers and other cyber staff located at corporate headquarters, and may have backup data stored at facilities managed by third parties. End users connected to a facility's cyber system may be scattered not only across the country, but even outside of the United States. As a result, facility cyber security often is not limited to the physical location of the facility itself. Good cyber security practices include a facility taking a holistic view of all its cyber assets, be they equipment, people, or data, and be they located on-site, at corporate headquarters, or elsewhere.

Interconnectivity of Critical and Seemingly Non-Critical Systems

Often, all of a facility's cyber systems will be interconnected in one form or another. As a result, some seemingly non-critical systems may warrant additional security attention as they are a potential avenue for access to the more critical systems that they are connected to. When analyzing the security posture of a critical system, it is important to identify all systems that are connected to it and review their security as well, as many times the security of the system is only as strong as its weakest link.

Impact of Risk Drivers

Much like in the world of physical security, the facility characteristics driving the risk have a great deal of impact on the appropriate cyber security posture for a facility. For example, if the facility is high-risk due to a release hazard, it likely needs to focus cyber security on its process control systems, as well as those cyber systems that assist in controlling access to the facility. However, if theft/diversion is the risk driver, then securing cyber business systems to ensure shipments and customers are proper may be more important than securing the process control systems.

Physical Security for Cyber Assets

Cyber systems can not only be compromised electronically, but also can be compromised physically. Protecting a server with an ID and password is not enough if someone can simply reach out and unplug it, or worse, pull a hard disk drive with sensitive data out of the machine and put it in their pocket. Accordingly, physically protecting critical cyber assets is typically a key component of a comprehensive cyber security program.

Marking and otherwise restricting specific physical areas in a facility can greatly improve security, as can guarding access to backup media and other external copies of data, especially when combined with a role based security model through which all personnel know exactly where they are and are not allowed. Also beneficial are measures to ensure that only authorized individuals are able to physically access sensitive IT areas, such as control rooms, LAN and server rooms, wiring closets, and workstations operating sensitive applications (e.g., access control or CCTV monitoring software).

Some examples of tools to physically restrict access include electronic access control, cipher locks, physical keys, visual control, and policy. Electronic access control is the most effective, followed by cipher locks, physical keys and visual control. Developing only a policy is the least effective but is still more desirable then having no controls. Suitability reviews and job assignment can be used to help identify which staff is granted access to certain restricted areas, equipment, and information. It is also a good practice for facilities to ensure that restricted IT areas cannot be accessed by going over or under the building's internal partitions such as via low-hanging panel ceilings or raised floors. Sensitive IT areas are best protected when bordered by true floor to true ceiling walls, or the areas above the ceiling or below the floor should be secured by wire partitions and/or alarmed to detect/prevent intrusion.

Layered Security

Completely adequate protection is rarely achievable solely through implementing a single security measure. Rather, the optimal security solution typically depends upon the use of multiple countermeasures providing "layers of security" for protection. This may include not only the layering of multiple physical protective measures, but also the effective integration of physical protective measures with procedural security measures, including procedures in place before an incident and those employed in response to an incident.

Managing External Service Providers

External service providers, business partners, and vendors could potentially present risk to an organization's cyber security. Good cyber security includes ensuring that partner organizations subject their personnel to security requirements acceptable to you if they are to have access to your facilities, systems, information, and intellectual property. Common tools to assist in this include memoranda of agreements, non-disclosure agreements, confidentiality agreements, and conflict of interest agreements.

Performance Standards Affected by Cyber Security Measures

Cyber security measures have the most direct impact on RBPS 8. Cyber security measures can secondarily impact RBPS 5, 6, 7, and 10.

Additional Resources on Cyber Security Measures

INFORMATION AND CYBER SECURITY	
RESOURCES	**SOURCES**
CERT: *Preventing Insider Sabotage: Lessons Learned from Actual Attacks,* by: Dawn Cappelli, November 14, 2005 - Carnegie Mellon University	www.cert.org/archive/pdf/InsiderThreatCSI.pdf
Cert-Coordination Center Survey Site-Index	www.cert.org
Computer Incident Advisory Capability , U.S. Department of Energy Office of Cyber Security	www.ciac.org/ciac/index.html
Computer Security Resources, U.S. Computer Emergency Readiness Team	www.us-cert.gov/resources.html
Cyber Security Alerts, U.S. Computer Emergency Readiness Team	www.us-cert.gov/cas/alerts/
Defense Information Systems Agency	www.disa.mil/main/prodsol/index.html
Effective Physical Security, Part Two, Equipment, Third Edition, Fennelly, Lawrence J., Butterworth-Heinemann, 1997 (ISBN: 0-7506-9873-X)	Available through numerous booksellers online
Incident Management, Carnegie Mellon University	https://buildsecurityin.us-cert.gov/portal/article/bestpractices/incident_management/overview.xml
Federal Financial Institutions Examination Council's (FFIEC) Information Security	www.ffiec.gov/ffiecinfobase/booklets/information_security/infosec_toc.htm
Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, National Threat Assessment Center, U.S. Secret Service	www.cert.org/archive/pdf/insidercross051105.pdf
Risk Management Guidelines for Information Technology Systems By	http://csrc.nist.gov/publications/nistpubs/800-

Gary Stoneburner, Alice Goguen and Alexis Feringa	30/sp800-30.pdf
Safeguarding your Technology. Practical Guidelines for Electronic Education Information Security, National Center for Education Statistics	http://nces.ed.gov/pubs98/safetech/index.asp
SANS Institute - Security Policy Projects- *Examples of Policies for Information / Cyber Security*	www.sans.org/resources/policies/
Handbook of Information Security Management, The CISSP Open Study Guides Web Site	www.cccure.org/Documents/HISM/ewtoc.html
The National Strategy to Secure Cyberspace	www.whitehouse.gov/pcipb/
The Security Portal for Information System Security Professionals, Information/Links & Suppliers for Network Security	www.infosyssec.com/infosyssec/physfac1.htm
Window Security.com - Articles and Tutorials	www.windowsecurity.com/articles_tutorials/

Security Procedures, Policies, and Plans

An effective facility security posture will incorporate a wide variety of security procedures policies, and plans. These procedures, policies, and plans typically will detail how a facility performs a myriad of security related tasks, including: (1) Inventory Controls/Product Stewardship; (2) Managing Control Points; (3) Screening; (4) Personnel Surety (i.e., Background Checks); (5) Exercises and Drills; (6) Training; and (7) Responding to Elevated Threat Levels.

Inventory Controls/Product Stewardship

Product stewardship is a term used to describe a product-centered approach to protection of potentially dangerous chemicals, such as chemicals of interest, calling for manufacturers, retailers, and consumers, to share responsibility for reducing the potential for theft, contamination, or misuse of such chemicals. Voluntary product stewardship activities have been taking place within the chemical industry for many years so inclusion as a component of the CFATS is the natural evolution of recommended business practice.

Types of Inventory Controls/Product Stewardship

Inventory controls can be used to track, for example, chemicals of interest at covered facilities from single stockrooms to large multi-site enterprise environments. Inventory control systems may differ in many respects, but generally could include the following elements:

- lists all the chemicals of interest at the facility
- provides tracking of the quantity and the physical location of each chemical
- monitors use by authorized personnel
- allows generation of reports listing chemicals of interest by location, vendor, name, etc.
- provides container-based tracking of multiple lots, vendors, and sizes
- tracks disposal and maintains a record of disposed containers
- purchasing/receiving record for materials management
- linked to MSDS information

Security Considerations for Inventory Controls/Product Stewardship

A properly utilized inventory control system can not only provide a level of security for COI, but in most cases can offer a financial benefit to the company by limiting interruptions in production due to lack of material or loss of sales due to limited stock. A good inventory control system will take into account raw materials, in-process or semi-finished materials, and finished goods ready for sale or transport.

A facility may want to consider limiting access to areas where dangerous chemicals such as theft COI are stored to authorized personnel only as a means of inventory control and may want to implement a system that requires anyone entering an area where theft COI are stored to both sign-in and sign-out could be utilized.

Physical barriers, such as fences and vehicle barriers may also be utilized as an effective means of inventory control. For example, by physically blocking access to an area where theft COI are stored a facility owner/operator can achieve a higher level of security related to that COI.

Maintaining quality records of sales, deliveries, and transfers can assist an owner/operator in maintaining control over the inventory. As part of maintaining accurate records an owner/operator may find it helpful to conduct regular on-site counts of all materials stored in a facility. For example, by conducting regular counts the owner/operator effectively controls inventory and is aware at any given time of the quantities of COI on-site.

Performance Standards Affected by Inventory Controls/Product Stewardship

The implementation of inventory controls/product stewardship can have a significant impact in helping a facility achieve RBPS 1,2,3,4,5,6 and to some extent 10.

Additional Resources on Inventory Controls/Product Stewardship

INVENTORY CONTROL SYSTEMS	
RESOURCES	**SOURCES**
Railroad Commission of Texas Case Study : Case study on the benefits of implementing an inventory control system	www.rrc.state.tx.us/divisions/og/key-programs/ogkwchgo.html
U.S. Small Business Administration, *Inventory Control Overview and Ideas*	www.ct-clic.com/Newsletters/customer-files/inventory0602.pdf

Managing Control Points

Control points, screening and parking security measures (in conjunction with other types of security measures) are the preferred and recommended solution to provide proper access control and meet the performance standards of the Access Control and Screening RBPS. Control points, screening and parking security measures could be implemented to meet the Access Control and Screening RBPS to address approach, denial, personnel identification, hand-carried items inspection, vehicle identification and vehicle inspections.

Because control systems are not self-administering, they should be periodically tested and policed. A typical procedure is the vulnerability test, or "created-error" check, in which an error or breach, such as an erroneous invoice, is deliberately planted in the system to see if it is detected and reported.

Table A3: Control Point Considerations	
Approach	**Denial**
• Traffic Calming – Reduce the speed of incoming vehicles (all Tiers) - Road alignment (circle, serpentine) - Drop-in or retractable bollards (to cause serpentine traffic	• Rejection point prior to facility access (Tiers 1, 2, & 3)

flow) - Barriers (all Tiers) □ Bollards □ Jersey Barriers or K-Rails - Speed bumps, tables, or serpentine approach (all Tiers) - Gates □ Not crash rated (Tier 4) □ K-4 (Tiers 3 & 4) □ K-6 (Tiers 2 & 3) □ K-8 (Tiers 1 & 2) □ K-10 (Tiers 1 & 2) □ K-12 or greater (Tier 1) • Identification (all Tiers) - Identify potential threat vehicles, including those attempting entry through the outbound lanes of traffic	

Types of Managing Control Points

Control point measures are measures used to help control vehicular access to a facility, by calming traffic as it approaches the facility, providing an opportunity for vehicle identification to occur, and by denying facility access to unauthorized vehicles. There are many different systems and policies that can effectively manage access to a facility. The individual owner / operator will need to consider the costs associated with each type of system as it relates to the COI stored / used at the facility. Control point measures include:

- Aligning roads in a manner to calm traffic (e.g., circles, serpentine roads)
- Bollards, barriers, K-Rails, etc. to cause serpentine traffic flow
- Speed bumps or tables
- Gates
- Identification points and rejection points prior to facility access

By limiting or managing parking on-site, a facility can help minimize ease of access to critical assets located inside the facility's perimeter. While completely prohibiting on-site parking is one option, less extreme measures are available, such as limiting on-site parking to certain vehicle classes—e.g., only "corporate" vehicles allowed on-site or only full-time employee vehicles allowed on-site (i.e., no visitor or contractor parking within the facility perimeter). Another option is to allow parking on-site, but locate it a significant distance away from the critical assets, and prevent means of vehicular egress to the critical assets.

Security Considerations for Managing Control Points

It is unlikely that any one type of control point management will be effective on its own, rather a combination of tools will likely need to be used. By layering a number of systems at a facility the owner / operator can increase security across a broader range of threats. A layered approach to asset security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

Performance Standards Affected by Managing Control Points

The implementation of procedures for the managing of control points can have a significant impact in helping a facility achieve RBPS 1,2,3,4 and to a lesser extent 8 and 12.

Additional Resources on Managing Control Points

MANAGING CONTROL POINTS	
RESOURCES	**SOURCES**
Security Industry Association: *Issues, Status and Trends*	www.securitymanagement.com/files/biometrics_physicalaccess0206.pdf
Security Guidelines for American Enterprises Abroad, US Department of State, Overseas Security Advisory Council, November 1994	www.state.gov/documents/organization/19790.pdf
Radio Frequency Identification (RFID) technology, University of Washington	www.cs.washington.edu/homes/suciu/PCSI-2007-05-0050.pdf

Screening

Through identification, screening, and inspection, a facility is better able to prevent unauthorized access to the facility and more likely to deter and detect unauthorized introduction or removal of substances and devices that may cause a dangerous chemical reaction, explosion, or hazardous release.

Types of Screening

A variety of different types of measures may be used to perform screening, such as personnel identification, hand-carried items inspections, vehicle identification, and vehicle inspections. A list of considerations for each type of screening is contained in Table A4 below, and additional details on each follow.

Table A4 – Screening Considerations Applicable to All Tiers

Personnel Identification	Hand-carried Items Inspection	Vehicle Identification	Vehicle Inspection
<u>Employees</u> Govt. issued photo ID Facility-specific photo ID electronic access control badge <u>Regular contractors</u> Govt. issued photo ID Company issued photo ID Facility-specific photo ID electronic access control badge	• Employees • Regular contractors • Temporary contractors • Visitors • Inspection may include: - Visual inspection - Use of	• Known shippers only • Authorized bill of lading • Facility-issued vehicle ID system	• Employee / contractor personal vehicles (POV) • Company vehicles • Contractor vehicles • Visitor vehicles • Delivery trucks • Vehicle inspection may include: - Visual inspection - Use of canines

Temporary contractors Govt. issued photo ID Company issued photo ID Facility-specific photo ID electronic access control badge Visitors Govt. issued photo ID Company issued photo ID Facility-specific photo ID electronic access control badge	canines (trained dogs) - Ionic explosives detection - X-ray inspection - Metal detectors		(trained dogs) - Under / over vehicle inspection systems - Cargo inspection systems

Personnel Identification

A primary component of successfully screening and controlling access is knowing who is allowed on-site. Personnel identification measures help a facility quickly determine whether or not an individual is permitted facility access, and certain identification measures can help both security officers and other employees quickly know whether or not an individual is authorized for facility access. Examples of personnel identification measures include:

- Conducting checks of government issued photo IDs prior to permitting facility access
- Providing company issued photo IDs to individuals permitted access to the facility, identifying:
  - Employees
  - Regular contractors
  - Temporary contractors
  - Visitors
- Providing facility-specific photo IDs to individuals permitted access to the facility, identifying:
  - Employees
  - Regular contractors
  - Temporary contractors
  - Visitors

Depending on the level of security desired, a facility may want to issue photo IDs (company or facility-specific) that are linked with electronic access control systems such as proximity ID readers or swipe access controls for an added layer of security. Electronic access control systems can be tailored to specific locations within a facility, thus providing the ability to limit access to restricted areas to authorized individuals. They also have the additional benefit of maintaining a record regarding who has accessed what areas.

A personnel identification system is most effective when used in conjunction with the performance of background checks and other personnel surety measures. Such measures are the focus of RBPS 12 – Personnel Surety.

Hand-Carried Items Inspection

A second element of a vigorous screening program is the inspection of items brought into the facility, whether brought in by employees, contractors, or visitors. Among other things, inspections may include:

- Visual inspections
- X-ray inspections
- Use of metal detectors
- Use of ionic explosives detection equipment
- Use of trained explosive detection canines

The type of inspection measures implemented, the thoroughness of inspections, and the frequency of inspections may vary based on a variety of factors, including the facility's tier (e.g., more vigorous and frequent measures may be suitable for higher tiers) and who is being inspected (e.g., more frequent and thorough inspections may be desired for visitors than for employees).

Vehicle Identification and Inspection

Another element of a comprehensive screening program is a vehicle identification and inspection program.

Vehicle identification measures can include using a facility-issued vehicle ID system (e.g., providing authorized vehicles with stickers or placards), using only known shippers and/or delivery companies, and requiring authorized bills of lading for access to the facility. These types of measures can help satisfy the standards established for RBPS 5 – Shipping, Receipt, and Storage, and are complemented by other measures recommended for RBPS 5 compliance.

Vehicle inspection measures that can be helpful in meeting the screening and access control standards include:

- Visual inspections
- Use of trained explosive detection canines
- Under/over vehicle inspection systems
- Cargo inspection systems

Much like hand-carried item inspections, the type of vehicle inspection measures implemented, the thoroughness of inspections, and the frequency of inspections may vary based on a variety of factors, including the facility's tier (e.g., more vigorous and frequent inspections may be suitable for higher tiers) and whose vehicle is being inspected (e.g., more frequent and thorough inspections may be desired for visitors or unscheduled delivery trucks than for employees or regularly scheduled deliveries).

Security Considerations for Screening

Layered Security

No matter the size of the individual asset being secured, completely adequate security likely will not be achievable through the deployment of a single protective measure; rather an optimal security solution typically involves the use of multiple protective measures providing "layers of security." Layering of security measures can be achieved in many different manners, such as:

- Incorporating different types of security measures (e.g., integrating physical protective measures, such as barriers, lighting, and electronic security systems with procedural security measures, such as procedures guiding how a security should respond to an incident)
- Using multiple lines of detection used to achieve protection-in-depth at critical assets
- Using complementary sensors with different means of detection (e.g., a CCTV and an intrusion detection system) to cover the same area.

A layered approach to asset security potentially increases the opportunity to use existing facility and natural features or more applicable technologies to meet the performance objectives at a reduced cost.

Physical and Environmental Considerations

When determining the selection and layout of asset security components, a facility owner/operator should take into consideration the physical and environmental characteristics surrounding the asset. Important *physical considerations* for evaluating the cost-effectiveness of countermeasures include:

- Asset size and asset perimeter length and convolution
- Terrain and urbanization
- Adjacent facilities and transportation corridors
- Approach angles and vehicle speeds
- Availability of supporting infrastructure

In addition to the physical considerations listed above, *environmental factors* also should be considered when making decisions regarding asset security, as certain environmental conditions can significantly affect sensor and lighting performance. For example, certain sensors or other IDS components that have near perfect detection capabilities during good weather might be subject to unacceptably high levels of false alarms during inclement weather (e.g., fog, rain, wind). Similarly, security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather. Accordingly, an owner/operator should consider the impact of environmental conditions when making determinations regarding security lighting and sensors or other IDS components.

Command and Control Considerations

Many asset security measures, such as intrusion detection systems or CCTV systems, consist of various hardware and software elements that can be operated or monitored effectively only by trained personnel, and owner/operators often will locate these functions in a command and control center. When designing command and control centers, owner/operators should consider merging security monitoring and reporting systems with other systems such as fire engineering reporting systems or process control. Technical merger of an active security system and a passive fire system may facilitate a common set of operational procedures (e.g., reporting, training, and emergency response), and prove a more cost-effective approach to overall facility safety and security management.

Performance Standards Affected by Screening

The implementation of screening can have a significant impact in helping a facility achieve RBPS 1, 2, 3, 4 and 6.

Additional Resources on Screening

SCREENING	
RESOURCES	**SOURCES**
U.S. Coast Guard Transportation Security Administration Transportation Port Worker, Interim Screening Program, April 25, 2006	www.uscg.mil/hq/g-m/mp/pdf/Part125GuidanceFinal.pdf
Technical Support Working Group	www.tswg.gov
The President's National Security Telecommunications Advisory Committee, Trusted Access Task Force: *Screening, Credentialing, and Perimeter Access Controls Report*, January 19, 2005	www.ncs.gov/nstac/reports/2005/Final%20TATF%20Report%2004-25-05.pdf

Personnel Surety/Background Checks

Background investigation: DHS believes personnel surety to be a key component of a successful chemical facility security program, with the level of screening commensurate with the access provided. Examining personnel backgrounds is the process of acquiring information on an individual through third-party services, government organizations, and private individuals to make a "suitability determination" for the future actions based upon past actions. Background investigation also verifies the accuracy of an applicant's employment history, educational history, and credentials, as well as confirming the lack of criminal history and sanctions. Such investigations rely primarily on public or private records to confirm or disprove the accuracy of an applicants' resume or job application. Because of the potential sensitivity of the information uncovered, background investigations are subject to a unique set of laws and regulations to protect employees and consumers in the event of misuse of data or fraud.

Types of Personnel Surety/Background Checks

The contents, type, and depth of background investigations vary widely. Most basic checks consist of at least the following elements:

a) Criminal record search
b) Employment verification
c) Education verification
d) Driving record
e) Credit check

In a due-diligence investigation, many additional elements could be added – from multi-jurisdictional civil searches to interviews with friends, family and neighbors. The level and depth of background investigations to reduce the likelihood of sabotage should be tied to the potential severity of the consequences that could occur because of sabotage, and applicable to individuals with potential access to the area or the specific asset capable of generating those undesired consequences.

There are a variety of types of investigative searches that can be used by employers or potential employers. Many commercial websites will offer specific searches to employers for a fee. Services like these typically will actually perform the background checks, supply the company with adverse action letters, and offer to ensure compliance with applicable legal requirements throughout the process. It is important to be selective about which pre-employment screening agency you use. A legitimate company should be willing to explain the process to you and should have some type of application process to ensure they are providing information to only legitimate businesses. Many employers choose to search the most common records, such as criminal records, driving records, and education verification themselves. Other searches such as sex offender registry, credential verification, reference checks, and credit reports are becoming increasingly common. Employers should consider the position in question when determining which types of searches to include, and typically should use the same types of searches for every applicant being considered for one position. Examples of searches that facilities may wish to consider under RBPS 12 include:

- Criminal History Searches: This typically involves searching multiple county, state and federal data repositories which contain criminal records of individuals entered into the respective system. County courts generally are the most comprehensive source of information for criminal activity. County search results provide criminal charges, dates, sentencing and disposition, for felonies and/or misdemeanors in the county seat court of the requested jurisdiction. Detailed dockets and supporting information are also available. Statewide repositories vary in detail and scope of information for each state. Data available may reflect arrest information obtained by police departments, county cases forwarded from local courts, or other criminal data housed by the state. Federal search results will provide information on criminal activity that occurred outside state or local jurisdiction and was prosecuted at the district court level. Personal identification requirements for criminal history searches may include: first name, middle initial, last name, date of birth, social security number, and the desired county to search. Release from the individual may be required prior to conducting this type of search.

- National Criminal Scan: This is an effective tool to screen applicants who have lived in numerous locations or whose previous positions required travel across state lines. This type of background check is recommended as a supplemental search to criminal history screening to identify criminal activity in jurisdictions outside of current and previous residence and employment geographical locations. Personal identification requirements for national criminal scan may include first name, middle name, last name, and date of birth.

- Social Security/Name Trace: This search reveals names associated with a social security number, past and present addresses, and fraudulent use of social security numbers. Results may be used to cross-reference addresses supplied by applicant to insure the integrity of the information on the job application or resume. Personal identification requirements for social security/name trace may include social security number, first name, middle initial and last name.

- Credit Report: This type of check is relevant for all security-related positions that involve access to cash, expensive equipment, or financial record keeping. This check provides the employer insight to the applicant's level of fiduciary responsibility. Personal identification requirements for credit repots include: social security number, first name, middle initial, last name, and address. Release from the individual may be required prior to conducting this type of search.

- Motor Vehicle Records (MVR): This screen is relevant for all security-related positions that may require the use of a motor vehicle. In some states, convictions of driving under the influence of drugs or alcohol are not revealed on the criminal record and are placed on the MVR. Motor vehicle reports include such items as DUI arrests and convictions, reckless behavior, moving violations, suspensions and revocations. Additionally, they outline the type of license approved and any restrictions to that license. These searches should comply with any applicable laws or rules, such as the Driver's Privacy Protection Act (DPPA). Personal identification requirements for this type of search include: social security number, first name, middle initial, last name, issuing state, license number, and date of birth. Release from the individual may be required prior to conducting this type of search.

- Personal References: This type of check is relevant for all applicants for any position with security implications. Key questions to references should address the following: dependability, adaptability, written and verbal communication, learning abilities, positive qualities, and areas for development. The reference should also have an opportunity to offer additional comments regarding the applicant. Personal identification requirements for this type of check include: first name, last name, maiden name (if applicable), reference name and phone number.

- Military Service Verification: This service is recommended for all applicants for any security-related position stating military service on job application or resume. This type of check is unique in that it provides information that is not normally found in employment and education screenings. This report provides such details as dates of service, rank, pay, decorations and medals, performance, and reason for discharge. Personal identification requirements for this type of search include: first name, middle

initial, last name, date of birth, military branch and location. Release from the individual may be required prior to conducting this type of search.

- Civil Court Records: Civil court records reveal if a person or company is involved in non-criminal lawsuits including litigation for tort, contract, or real estate disputes. The data typically comes directly from the individual counties and contains filings of court cases containing all plaintiffs, defendants, case numbers, date of filings, and judgment.

- Education Confirmation: This type of check is relevant for all applicants for security-related positions. Level of education is one of the most common item falsified on a job application or resume. Checks should verify academic credentials at all institutions including high school, college, and technical and trade schools. Checks should also provide verification of attendance, degrees, course certifications, GPA's, honors, course of study, and dates attended. Personal identification requirements for this type of search include: first name, middle initial, last name, maiden name if applicable, date of birth, social security number, institution name, state, years attended and degree received. Release from the individual may be required prior to conducting this type of search.

- Employment Verification: This type of check is relevant for all applicants for security-related positions due to the fact that employment history is often embellished. Employment checks verify present and past employment, including wages, dates of employment, job title and responsibilities. These results can also provide information on work habits, interaction with others, disciplinary actions, attendance, and eligibility for re-hire. Personal identification requirements for this type of search includes: first name, last name, maiden name (if applicable), social security number, employer's name and employer's state. The employer may require a signed release. Additional information provided, such as dates employed, position title, and reason for separation can be used to further validate the information provided by the applicant.

An example of a typical background check under RBPS 12 could include the following:

- Verification of social security number.
- Name and address of each employer and the period employed providing information on job title, responsibilities, overall job performance, reason for departure and eligibility for re-hire.
- Confirmed dates of high school attendance. For applicants who attended college, verify dates of attendance, and credits or degrees earned.
- A search of federal, state, and county records in all jurisdictions in which the individual has worked or resided during the previous seven (7) years, including all geographical areas listed on the application, resume, and the social security number address verification report. The records search includes federal, state, county (or equivalent) felony and misdemeanor convictions, deferred adjudication, pleas of no contest, and unresolved indictments or other charges of crimes or offenses, except to the extent consideration of any such categories are prohibited by applicable law. Minor traffic offenses are not generally relevant; however, DWI/DUI is relevant and reported.
- For employees that whose job responsibilities involve operating motor vehicles - Information from the Department of Motor Vehicles in, but not limited to, the geographic

areas listed on the application, resume, or social security number address verification; to reveal violations and convictions.
- All employees and resident contractors whose job responsibilities involve financial or security responsibilities go through credit verification to show debt load, payment history, and information on civil actions such as judgments, liens, collections, or bankruptcies.
- E-verify or USCIS Form I-9.
- Screening for terrorist ties through the Terrorist Screening Database, as provided by the Department.

Examples of background check anomalies that a facility could consider significant under appropriate circumstances include:

- Individual is under indictment or information for, or who has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year;
- Individual is a fugitive from justice;
- Individual is an unlawful user of or addicted to any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802) and § 555.11);
- Individual has been adjudicated as a mental defective or has been committed to a mental institution;
- Individual may be denied admission to the United States or removed from the United States under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.);
- Individual has been discharged from the armed forces under dishonorable conditions;
- Individual having been a citizen of the United States, has renounced citizenship;
- Individual has been convicted within the preceding 7-year period of a felony or found not guilty by reason of insanity of a felony;
- Individual is a terrorism security risk to the United States;
- Individual has been released from incarceration within the preceding 5-year period for committing a felony.

Security Considerations for Personnel Surety/Background Checks

An "adjudicative" process is an examination by a company or facility of a sufficient amount of data, collected from one or more of the types of background checks previously discussed, to make an affirmative determination that the person is suitable for employment. This process is the careful weighing of a number of variables known as the 'whole person' concept. Available, reliable and relevant information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator typically considers factors such as:

a) The nature, extent, and seriousness of the conduct
b) The circumstances surrounding the conduct, to include knowledgeable participation
c) The frequency and recency of the conduct
d) The individual's age and maturity at the time of the conduct
e) The voluntariness of participation
f) The presence or absence of rehabilitation and other pertinent behavioral changes
g) The motivation for the conduct
h) The potential for pressure, coercion, exploitation, or duress
i) The likelihood of continuation or recurrence.

Each case should be judged on its own merits, and final determination remains the responsibility of the facility.

Visitor controls: Physical-security precautions include the screening, identification, and control of visitors. Visitors are generally classed in the following categories:

- Persons with whom the covered facility has business (such as suppliers, customers, and inspectors)
- Individuals or groups who desire to visit a covered facility for personal or educational, technical, or scientific reasons.
- Individuals or groups specifically sponsored by or representing the government
- Guided tours to selected portions of the covered facility in the interest of public relations

Certain actions can mitigate the risks posed by visitors. While background checks cannot identify all visitors who pose a risk, they are a valuable tool for alerting management of situations that may warrant more attention and control. Identification and control mechanisms for visitors should be in place. They may include the following:

- Positive identification of visitors
- Contacting facility personnel to validate the visit
- The use of visitor registration forms to provide a record of the visitor and the time, location, and duration of his visit
- The use of visitor cards/badges
- Visitor escort requirements

Individual visitors or groups of visitors entering a restricted area should meet specific prerequisites before being granted access.

Performance Standards Affected by Personnel Surety/Background Checks

The implementation of personnel surety/background checks can have a significant impact in helping a facility achieve RBPS 7 and 12.

Additional Resources on Personnel Surety/Background Checks

BACKGROUND CHECKS	
RESOURCES	**SOURCES**
Employee Background Screening, ASIS International	www.asisonline.org/guidelines/guidelinespreemploy.pdf
Personnel& Training CIP-004, NERC	www.nerc.com/pub/sys/all_updl/standards/rs/CIP-004-1.pdf
Pre-Employment Background Screening Guidance on Developing an Effective Pre-Employment Background Screening Process, FDIC	www.fdic.gov/news/news/financial/2005/fil4605a.html

Exercises and Drills

High-risk chemical facilities should develop a security awareness and training program that includes all level of facility personnel, including executives, management, operational, and technical employees. The program should include: policy, guidance and standards; training courses and materials; exercises of varying types and scope designed to improve the overall organizational deterrence, detection, delay and response capability to security and/or other emergency situations; a schedule; and evaluation and remedial action programs. Objectives of a security awareness and training program may include:

- Validate plans, policies and procedures
- Ensure that personnel are familiar with alert, notification, deployment and other related security procedures

Several aspects are generally important for a facility to implement a successful security awareness and training program, to include the need to train, exercise, drill, and test all facility employees on security.

A Security Awareness and Training Program is a predefined and documented set of scheduled activities, which include training, exercises, drills, tests and joint initiatives that focus on relevant security related issues for the facility and enhance the overall security awareness of all facility employees.

As part of the facility's security awareness and training program, training typically consists of a predefined and documented set of scheduled activities, which may include a deliberate blend of hands-on activities, seminars, orientations, workshops, on-line or interactive programs, briefings and lectures, that focus on relevant security related issues for the facility and enhance the overall security awareness of all facility employees.

Regularly scheduled training should be conducted to assure the readiness of all facility personnel. Training plans are developed and implemented to prepare individuals and groups (i.e., protective forces) to accomplish certain tasks, using selected equipment, under specific scenarios. This training may encompass a deliberate blend of hands-on activities, seminars, orientations, workshops, on-line or interactive programs, briefings and lectures.

Types of Exercises and Drills

As part of the facility's security awareness and training program, exercises should consist of a predefined and documented set of scheduled activities that represent a realistic rehearsal or simulation of an emergency that promote preparedness, improve the response capability of individuals, validate plans policies and procedures. Exercises may include a deliberate blend of tabletop exercises, functional exercises and full-scale exercises that focus on relevant security related issues for the facility and enhance the overall security awareness of all facility employees.

Exercises typically are conducted for the purpose of validating elements, both individually and collectively, of a facility's security posture and response capability. An exercise should be a realistic rehearsal or simulation of an emergency, in which individuals and organizations demonstrate the tasks that would be expected of them in a real emergency. Exercises generally should provide emergency simulations that promote preparedness, improve the response capability of individuals and organizations, validate plans, policies, procedures and systems, and determine the effectiveness

of the command, control and communication functions and event-scene activities. Exercises may vary in size and complexity to achieve their respective purposes.

The evaluation of an exercise typically should identify systemic weaknesses and suggest corrective actions that will enhance facility preparedness and response. Following an exercise, a comprehensive debriefing and after-action report should be completed. All data collected should be incorporated into a remedial action plan that provides input for annual revisions.

Drills are a coordinated, supervised activity normally used to exercise a single specific operation or function. Drills are also used to provide training with new equipment, to develop new policies or procedures, or to practice and maintain current skills.

As part of the facility's security awareness and training program, tests could consist of a predefined and documented set of scheduled activities, which may include a deliberate blend of static tests, dynamic tests and functional tests that focus on relevant security related issues for the facility and enhance the overall security awareness of all facility employees.

Testing is the technique of demonstrating the correct operation of all equipment, procedures, processes and systems that support the security infrastructure. The testing process validates that the equipment and systems conform to specifications and operate in the required environments and that procedures and processes are viable. Testing is used as a verification and validation technique to confirm that backup equipment and systems closely approximate the operations of the primary equipment and systems. Based on the measures and benchmarks desired, there are a variety of methods that can be used to test the functionality of backup environments, including:

- **Tabletop Exercise:** Tabletop exercises simulate an emergency situation in an informal, stress-free environment. They are designed to elicit constructive discussion as participants examine and resolve problems based on existing plans. There is minimal attempt at simulation, no utilization of equipment or deployment of resources, and no time pressures. The success of these exercises is largely determined by group participation in the identification of problem areas. They provide an excellent format to use in familiarizing newly assigned/appointed security personnel and senior security officials with established or emerging concepts and or plans, policies, procedures, systems and facilities.
- **Functional Exercises:** Functional exercises are fully simulated interactive exercises. They validate the capability of a group (i.e. protective force) or facility to respond to a simulated event testing one or more procedures and/or function of the facility's security plan. Functional exercises focus on policies, procedures, roles and responsibilities of single or multiple security functions before, during or after a security related event.
- **Full-Scale Exercises:** Full-Scale exercises simulate an actual security event. They are field exercises designed to evaluate the operational capabilities of the facilities security measures (i.e. physical measures and procedural measures) in a highly stressful environment. This realism can be accomplished through mobilization and response of facility personnel, equipment and resources.
- S**tatic Tests:** Static tests determine if all essential components of the equipment and systems are in place and meet the specification and design requirements of the facility.

- **Dynamic Tests:** Dynamic tests verify that all of the equipment and systems function independently of each other, function in consort with each other and satisfy the operational requirements of the organization.
- **Functional Tests:** Functional tests verify that the procedures for operating the equipment and systems in the backup environment are correct. This testing assures that when trained and qualified personnel utilize the backup equipment and systems, the instructions for operations are clear and complete.

Security Considerations for Exercises and Drills

As part of the facility's security awareness and training program, and a sub-set or type of exercise, drills generally consist of a predefined and documented set of scheduled activities that are used to exercise a single specific operation or function and can also be used to provide training with new equipment, to develop new policies or procedures, or to practice and maintain current skills.

Performance Standards Affected by Exercises and Drills

The implementation of exercises and drills can have a significant impact in helping a facility achieve RBPS 9 and 11.

Additional Resources on Exercises and Drills

EXERCISES/DRILLS/TESTS	
RESOURCES	**SOURCES**
ASIS Disaster Preparation Guide, 2003	www.asisonline.org/newsroom/crisisResponse/disaster.pdf
DHS Ready Business Emergency Planning Guide & Fact Sheet to Small to Mid-sized Businesses	www.asisonline.org/newsroom/crisisResponse/103105readybiz.pdf
On-Scene Commander's Guide for Responding to Biological/Chemical Threats, November 1, 1999, National Domestic Preparedness Office	www.au.af.mil/au/awc/awcgate/ndpo/oscg_ndpo.pdf
Security Awareness, training course from US Dept. of Transportation, for DOT Hazmat Employees, under HM-232	www.hazmatschool.com/descriptions/DOT_1362_information.html

Training

The length of the training and the depth of the coverage of the information provided and discussed will vary based on the audience and method of training selected. Typically, if the audience is designated security personnel, details of security procedures, operations, communications, etc., warrant extended discussion. Awareness training for the entire workforce might include topics such as incident identification and notification. Major topics or components of a training syllabus could include:

- Overview of the security awareness and training program
- Description of the facility's security organization
- Roles and responsibilities
- Identification of a security incident

- Notification of a security incident
- Response to a security incident
- Security related standard operating procedures
- Relationship with local response entities

Types of Training

Typically, a facility's security awareness and training program consists of a predefined and documented set of scheduled activities, which may include a deliberate blend of hands-on activities, seminars, orientations, workshops, on-line or interactive programs, briefings and lectures that focus on relevant security related issues for the facility and enhance the overall security awareness of all facility employees.

To maximize the benefit of a security awareness and training program, training topics should be tailored to specific classes of employees, as not all facility employees need the same level of training. For example, detailed training on security procedures, operating security equipment, security response protocols, and security laws and regulations may not be worthwhile for employees who do not have specific security responsibilities. Conversely, certain topics such as incident identification and notification are beneficial for the entire workforce to be trained on. Table A5 below provides a list of various training topics and the individuals within the organization who are most likely to benefit from that training.

Table A5 – Suggested Training Requirements

Training Topic	SSO/Asst SSO	Personnel with Security Responsibilities	All Remaining Employees
Security Laws and Regulations	XX		
Threats	XX		
Security Organization/Duties and Responsibilities	XX		
CSAT Components ▪ Top Screen ▪ SVA ▪ SSP ▪ Personnel Screening Database	XX		
Security Measures and Management of SSPs	XX		
Requirements for SSP	XX		
Drills and Training	XX		
Inspections and Screening	XX		
Recordkeeping	XX		
Knowledge of current security threats and patterns	XX	XX	
Recognition and detection of dangerous substances and devices ▪ Recognizing explosive materials ▪ Recognizing explosive devices ▪ Improvised explosives (e.g., using industrial materials) ▪ VBIEDs ▪ Hand-carried weapons ▪ Surveillance devices (e.g., camera phones	XX	XX	XX

Table A5 – Suggested Training Requirements			
Training Topic	**SSO/Asst SSO**	**Personnel with Security Responsibilities**	**All Remaining Employees**
Recognition of suspicious behavior	XX	XX	XX
Techniques used to circumvent security measures	XX	XX	XX
Crowd and traffic management and control techniques	XX	XX	
Security related communications	XX	XX	
Knowledge of emergency procedures, contingency plans, and crisis management plans	XX	XX	
CVI certification	XX	XX	
Operation of security equipment and systems	XX	XX	
Testing, calibration, and maintenance of security equipment and systems	XX	XX	
Relevant provisions of the SSP	XX	XX	XX
Methods of physical screening of persons and personal effects	XX	XX	
The meaning and the consequential requirements of the different DHS Threat Levels in general	XX	XX	XX

Security Considerations for Training

Frequency of Training, Drills, and Exercises. How frequently a facility chooses to conduct training, drills, and exercises likely will depend on a variety of factors. Such factors include the facility's risk tier, the training topic, the composition of the training's target audience, and the size of the facility. Table A6 below provides some recommended frequencies for various types of training, drills, and exercises by Tier.

Table A6 – Recommended Frequency (by Tier) of Sample Activities Under RBPS 11				
Activity	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Testing of alert, notification and activation procedures	Monthly	Quarterly	Semi-annual	Semi-annual
Testing of communications capability	Monthly	Quarterly	Semi-annual	Semi-annual
Security awareness briefing (or other means of refresher for the entire workforce) and pre-employment for all new or temporary workers	Annual	Annual	Annual	Annual
Training for protective force personnel	Quarterly	Quarterly	Semi-annual	Annual
Training for management personnel	Annual	Annual	Annual	Annual
Drills	Quarterly	Quarterly	Quarterly	Semi-Annual
Tabletop exercise	Bi-annual (alternate annually with full scale exercises)	Tri-annual (alternate every 18 months with full scale exercises)	Bi-annual	Tri-annual
Functional exercise	Annual	Annual	Bi-annual	Bi-annual
Full scale exercise (with local law enforcement and first responders)	Bi-Annual (alternate annually with tabletop exercises)	Tri-annual (alternate every 18 months with tabletop exercises)	N/A	N/A

Performance Standards Affected by Training

The implementation of monitoring systems can have a significant impact in helping a facility achieve RBPS 1, 2, 3, and 4, and 11.

Additional Resources on Training

TRAINING	
RESOURCES	**SOURCES**
Private Security Officer Selection and Training Guideline, ASIS International, 2004	www.asisonline.org/guidelines/guidelinesprivatedraft.pdf
Security Planning and Disaster Recovery. Maiwald, Eric and William Sieglend. 2002, American Public Works Association (APWA) (ISBN: 007222830X)	Available through numerous booksellers online
Information Guide for Responsible Care, Security Code of Management Practices, *Site Security & Verification*, July 2002	www.americanchemistry.com
Information Guide for Responsible Care, Security Code of Management Practices, *Value Chain Activities*, September 2002	www.americanchemistry.com
Emergency Preparedness Checklist, Federal Emergency Management Agency (FEMA), 1997	www.fema.gov/pdf/library/epc.pdf

Additional Resources

GENERAL RESOURCES	
RESOURCES	**SOURCES**
Protection of Assets Manual, ASIS International	http://www.protectionofassets.com/ (Access available through: www.asisonline.org)
Security Toolkit, Case Studies, Guidelines, Report and White Papers Information and guidance ASIS security experts	www.asisonline.org/toolkit/toolkit.xml
Chemical Group Security Assessment and Best Practices Report, New Jersey Domestic Security Preparedness Taskforce, Infrastructure Advisory Committee, April 30, 2003	www.state.nj.us/dep/rpp/brp/security/downloads/NJ%20Best%20Practices%20Chemical%20Sector.pdf
Chemical Site Security Vulnerability Assessment Model & Manual, Synthetic Organic Chemical Manufacturers Association (SOCMA)	www.socma.org/Products/VulnerabilityAnalysis.htm
Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report GAO-04-354, US General Accounting Office, March 30, 2004	www.gao.gov/new.items/d04354.pdf
Department of Army Field Manual FM-3-19.30 - Physical Security, January 8, 2001	www.globalsecurity.org/military/library/policy/army/fm/3-19-30/index.html
Effective Physical Security, Part Two, Chapter 8, Security Lighting, Third Edition, Fennelly, Lawrence J., Butterworth-Heinemann, 1997 (ISBN: 0-7506-9873-X)	Available through numerous booksellers online
Enhancing Security of Hazardous Materials Shipment Against Acts of Terrorism or Sabotage Using RSPA's Risk Management Self-Evaluation Framework (RMSEF), US Department of Transportation, January 2002	http://hazmat.dot.gov/riskmgmt/rmsef/rmsef_security_template.pdf
Fox, Jack. 2003. "Pipeline Infrastructure Security." July 13-16, Baltimore, Maryland. Reston, VA/ASCE, 0-7844-0690-1, 1817 pp., 2 vol.	www.pubs.asce.org/WWWdisplay.cgi?0301702
American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety, *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, August, 2002	www.aiche.org/Publications/pubcat/listings/081690877X.aspx
Heller, Miriam. 2003. "Infrastructure Security, Dependencies, and Asset Management." July 13-16, Baltimore, Maryland. Reston, VA/ASCE, 0-7844-0690-1, 1817	www.pubs.asce.org/WWWdisplay.cgi?0301782
Introduction to Security, Sixth Edition, Robert J. Fischer, Gion Green, Butterworth-Heinemann, 1998 (ISBN: 0-7506-9860-8)	Available through numerous booksellers online
US Joint Chiefs of Staff, *"Joint Tactics, Techniques and Procedures for Antiterrorism,"* Joint Pub 3-07.2, March 1998	www.fas.org/irp/doddir/dod/jp3_07_2.pdf
National Gas Utility Sector Critical Infrastructure Protection, American Gas Association, February 2005	www.aga.org
Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, FEMA 427, December 2003	www.fema.gov/plan/prevent/rms/rmsp427
Recommended Security Guidelines for Facilities, Navigation and Vessel Inspection Circular No. 11-02	www.uscg.mil/hq/g-m/nvic/11-02.pdf

(NVIC 11-02), January 13, 2003	
Risk Analysis and the Security Survey, James F. Broder, CPP, Butterworth-Heinemann, 2000 (ISBN: 0-7506-7089-4)	Available through numerous booksellers online
"*Application of Integrated Control Systems for Improved Protection,*" Rostami, Jamal and H. Besharatian. 2003, July 13-16, Baltimore, Maryland. Reston, VA/ASCE, 0-7844-0690-1, 1817 pp., 2 vol.	www.pubs.asce.org/WWWdisplay.cgi?0301724
Security Guidelines for American Enterprises Abroad, US Department of State, Overseas Security Advisory Council, November 1994	www.state.gov/documents/organization/19790.pdf
Security Management On-Line	www.securitymanagement.com
The Design and Evaluation of Physical Protection Systems, Garcia, Mary Lynn, Butterworth-Heinemann, 2001 (ISBN: 0-7506-7367-2)	Available through numerous booksellers online
The Security Portal for Information System Security Professionals, Information/Links & Suppliers for Security	www.infosyssec.com/infosyssec/physfac1.htm
Threat Advisory System Response Guideline, ASIS International, 2004	www.asisonline.org/guidelines/guidelinesthreat.pdf
Unified Facilities Criteria: Design and O&M: Mass Notification Systems, US Department of Defense, December 2002	www.wbdg.org/ccb/DOD/UFC/4_021_01.pdf
Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF), 2002	Sandia National Laboratories
Security Planning and Design, Demkin, Joseph A., ed., The American Institute of Architects, Wiley, 2003 (ISBN: 047127156X)	Available through numerous booksellers online
Building Security: Handbook for Architectural Planning and Design, Nadel, Barbara A, FAIA, McGraw-Hill Professional, 2004 (ISBN: 0071411712)	Available through numerous booksellers online

CORPORATE SECURITY POLICIES AND SECURITY POLICY ADMINISTRATION	
RESOURCES	**SOURCES**
Responsible Care© Security Code of Management Practices, American Chemistry Council	www.americanchemistry.com/s_acc/bin.asp?CID=373&DID=1255&DOC=FILE.PDF"
Security Guidelines for the Petroleum Industry, American Petroleum Institute, April 2003.	www.api.org/policy/otherissues/upload/SecurityGuideEd3.pdf
Threat Advisory System Response Guideline, Considerations and Potential Actions in Response to the Department of Homeland Security Advisory System, ASIS International, 2004	www.asisonline.org/guidelines/guidelinesthreat.pdf
Mail Center Security Guide, Publication 166, US Postal Service	www.usps.com/cpim/ftp/pubs/pub166/welcome.htm

SECURITY AWARENESS AND TRAINING	
RESOURCES	**SOURCES**
ASIS Disaster Preparation Guide, 2003	www.asisonline.org/newsroom/crisisResponse/disaster.pdf
National Security Institute: *Bomb Threats and Physical Security Planning*	http://nsi.org/library/terrorism/bombthreat.html
DHS Ready Business Emergency Planning Guide & Fact Sheet to Small to Mid-sized Businesses	www.asisonline.org/newsroom/crisisResponse/103105readybiz.pdf
Emergency Preparedness Checklist, Federal Emergency	www.fema.gov/pdf/library/epc.pdf

Management Agency (FEMA), 1997	
Information Guide for Responsible Care, Security Code of Management Practices, *Value Chain Activities*, September 2002	www.americanchemistry.com
Information Guide for Responsible Care, Security Code of Management Practices, *Site Security & Verification*, July 2002	www.americanchemistry.com
On-Scene Commander's Guide for Responding to Biological/Chemical Threats, November 1, 1999, FBI: National Domestic Preparedness Office	www.au.af.mil/au/awc/awcgate/ndpo/oscg_ndpo.pdf
Security Awareness, training course from US Dept. of Transportation, for DOT Hazmat Employees, under HM-232,	www.hazmatschool.com/descriptions/DOT_1362_information.html
Chapter 8 - Security Design, *Facilities Standards for the Public Building Service*	www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/p100-2003c8_R2E-qD-b_0Z5RDZ-i34K-pR.pdf
Security Planning and Disaster Recovery. Maiwald, Eric and William Sieglend. 2002, American Public Works Association (APWA) (ISBN: 007222830X)	http://www.aiche.org/Publications/pubcat/listings/081690877X.aspx
Chief Security Officer Guideline, ASIS International, 2004	www.asisonline.org/guidelines/guidelineschief.pdf
Private Security Officer Selection and Training Guideline, ASIS International, 2004	www.asisonline.org/guidelines/guidelinesprivatedraft.pdf
"*Company Security Officer*," 2003 Edition, International Maritime Organization	www2.imo.org/b2c_imo/b2c/init.do
"*Guarding America: Security Guards and U.S. Critical Infrastructure*," Parfomak, Paul W., Congressional Research Service, Nov. 12, 2004	www.fas.org/sgp/crs/RL32670.pdf